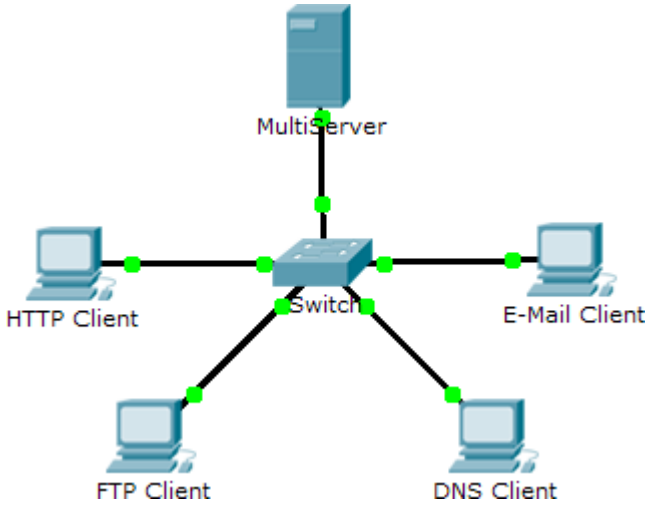
Packet Tracer Simulation - TCP and UDP Communications

Topology



Objectives

Part 1: Generate Network Traffic in Simulation Mode

Part 2: Examine the Functionality of the TCP and UDP Protocols

Background

This simulation activity is intended to provide a foundation for understanding the TCP and UDP in detail. Simulation mode provides the ability to view the functionality of the different protocols.

As data moves through the network, it is broken down into smaller pieces and identified in some fashion so that the pieces can be put back together. Each of these pieces is assigned a specific name (protocol data unit [PDU]) and associated with a specific layer. Packet Tracer Simulation mode enables the user to view each of the protocols and the associated PDU. The steps outlined below lead the user through the process of requesting services using various applications available on a client PC.

This activity provides an opportunity to explore the functionality of the TCP and UDP protocols, multiplexing and the function of port numbers in determining which local application requested the data or is sending the data.

Part 1: Generate Network Traffic in Simulation Mode

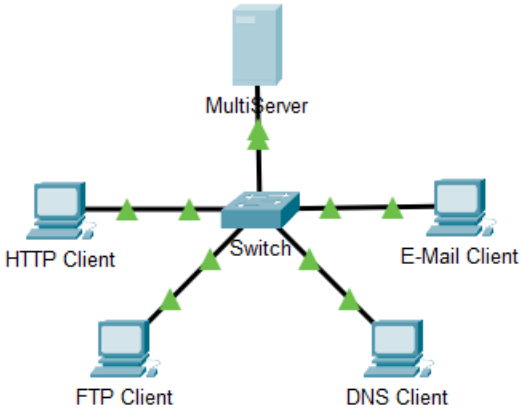
Step 1: Generate traffic to populate Address Resolution Protocol (ARP) tables.

Perform the following tasks task to reduce the amount of network traffic viewed in the simulation.

a. Click **MultiServer** and click the **Desktop** tab > **Command Prompt**.

b. Enter the **ping 192.168.1.255** command. This will take a few seconds as every device on the network responds to **MultiServer**.

c. Close the **MultiServer** window.



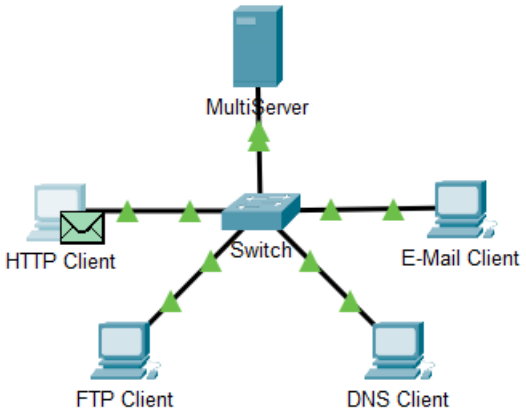
Step 2: Generate web (HTTP) traffic.

a. Switch to Simulation mode.

b. Click **HTTP Client** and click the **Desktop** tab > **Web Browser**.

c. In the URL field, enter **192.168.1.254** and click **Go**. Envelopes (PDUs) will appear in the simulation window.

d. Minimize, but do not close, the **HTTP Client** configuration window.

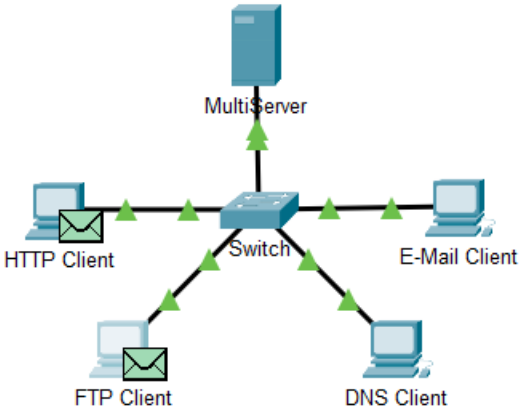


Step 3: Generate FTP traffic.

a. Click **FTP Client** and click the **Desktop** tab > **Command Prompt**.

b. Enter the **ftp 192.168.1.254** command. PDUs will appear in the simulation window.

c. Minimize, but do not close, the **FTP Client** configuration window.

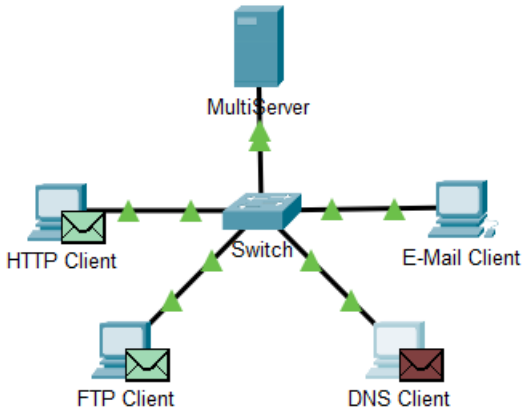


Step 4: Generate DNS traffic.

a. Click **DNS Client** and click the **Desktop** tab > **Command Prompt**.

b. Enter the **nslookup multiserver.pt.ptu** command. A PDU will appear in the simulation window.

c. Minimize, but do not close, the **DNS Client** configuration window.



Step 5: Generate Email traffic.

a. Click **E-Mail Client** and click the **Desktop** tab > **E Mail** tool.

b. Click **Compose** and enter the following information:

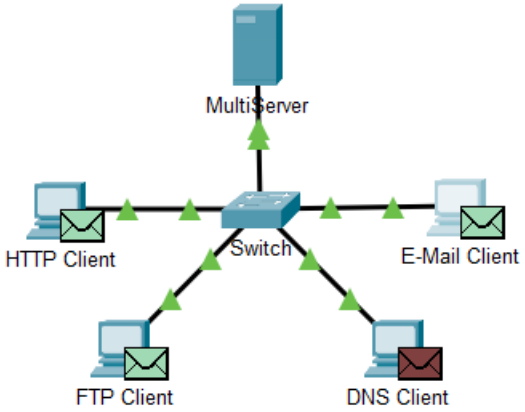
1) **To:** user@multiserver.pt.ptu

2) **Subject:** Personalize the subject line

3) **E-Mail Body:** Personalize the Email

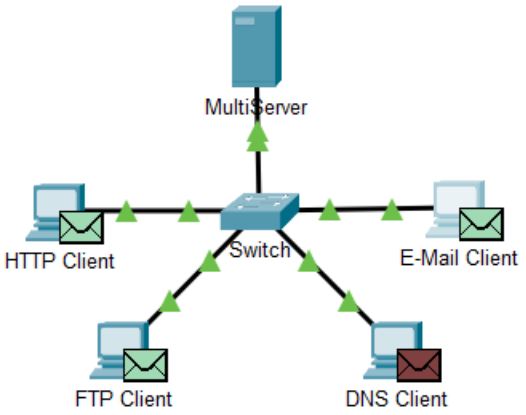
c. Click **Send**.

d. Minimize, but do not close, the **E-Mail Client** configuration window.



Step 6: Verify that the traffic is generated and ready for simulation.

Every client computer should have PDUs listed in the Simulation Panel.

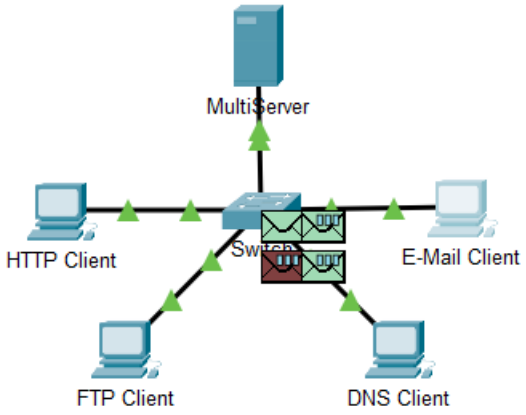


Part 2: Examine Functionality of the TCP and UDP Protocols

Step 1: Examine multiplexing as all of the traffic crosses the network.

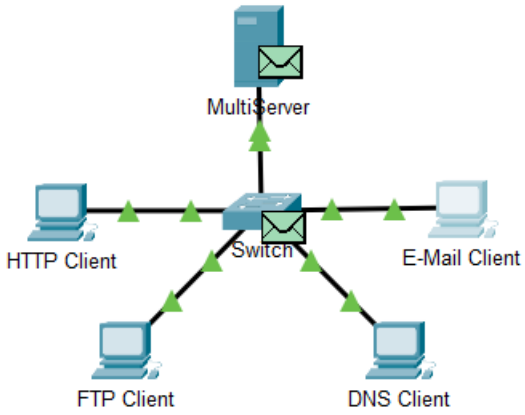
You will now use the **Capture/Forward button** and the **Back** button in the Simulation Panel.

a. Click **Capture/Forward** once. All of the PDUs are transferred to the switch.



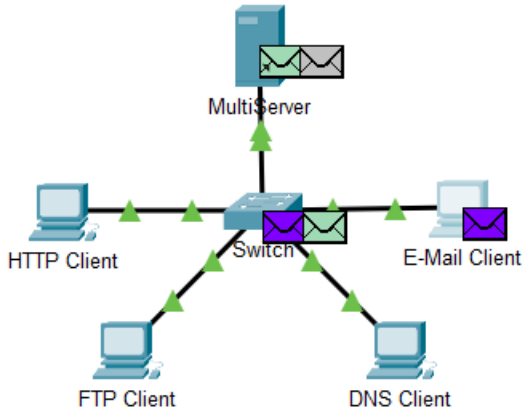
b. Click **Capture/Forward** again. Some of the PDUs disappear. What do you think happened to them?

The PDUs disappear have been stored in the Switch.



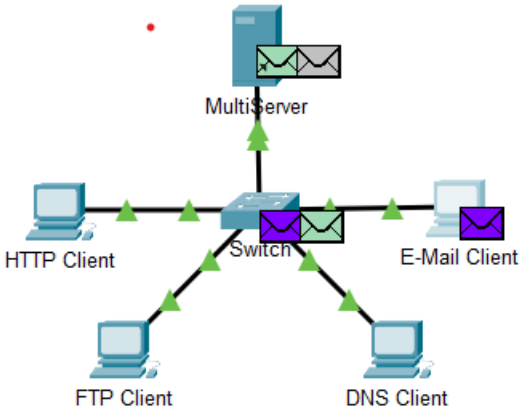
c. Click **Capture/Forward** six times. All clients should have received a reply. Note that only one PDU can cross a wire in each direction at any given time. What is this called?

Multiplexing.

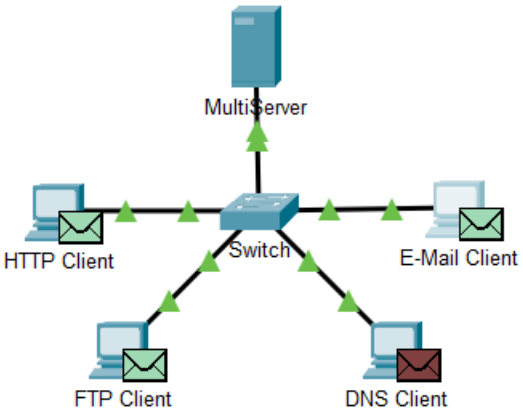


d. A variety of PDUs appears in the event list in the upper right pane of the simulation window. Why are they so many different colors?

Different color of PDUs represent different type of protocol.



e. Click **Back** eight times. This should reset the simulation.



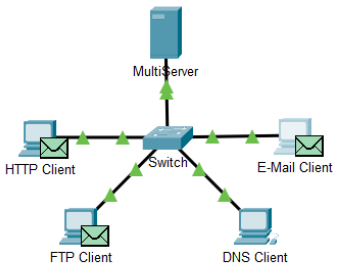
Note: Do not click **Reset Simulation** any time during this activity; if you do, you will need to repeat the steps in Part 1.

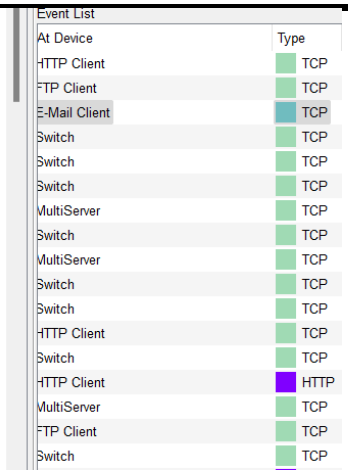
Step 2: Examine HTTP traffic as the clients communicate with the server.

a. Filter the traffic that is currently displayed to display only **HTTP** and **TCP** PDUs filter the traffic that is currently displayed:

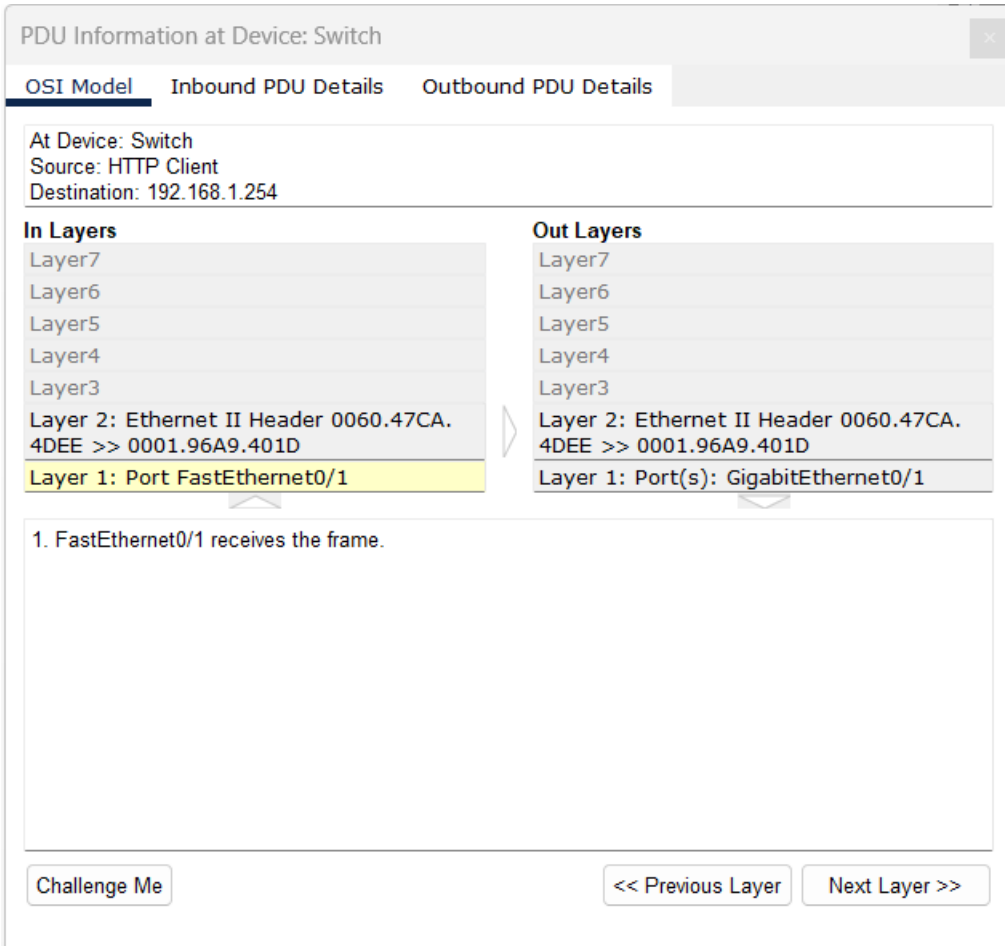
1) Click **Edit Filters** and toggle the **Show All/None** check box.

2) Select **HTTP** and **TCP**. Click anywhere outside of the Edit Filters box to hide it. The Visible Events should now display only **HTTP** and **TCP** PDUs.





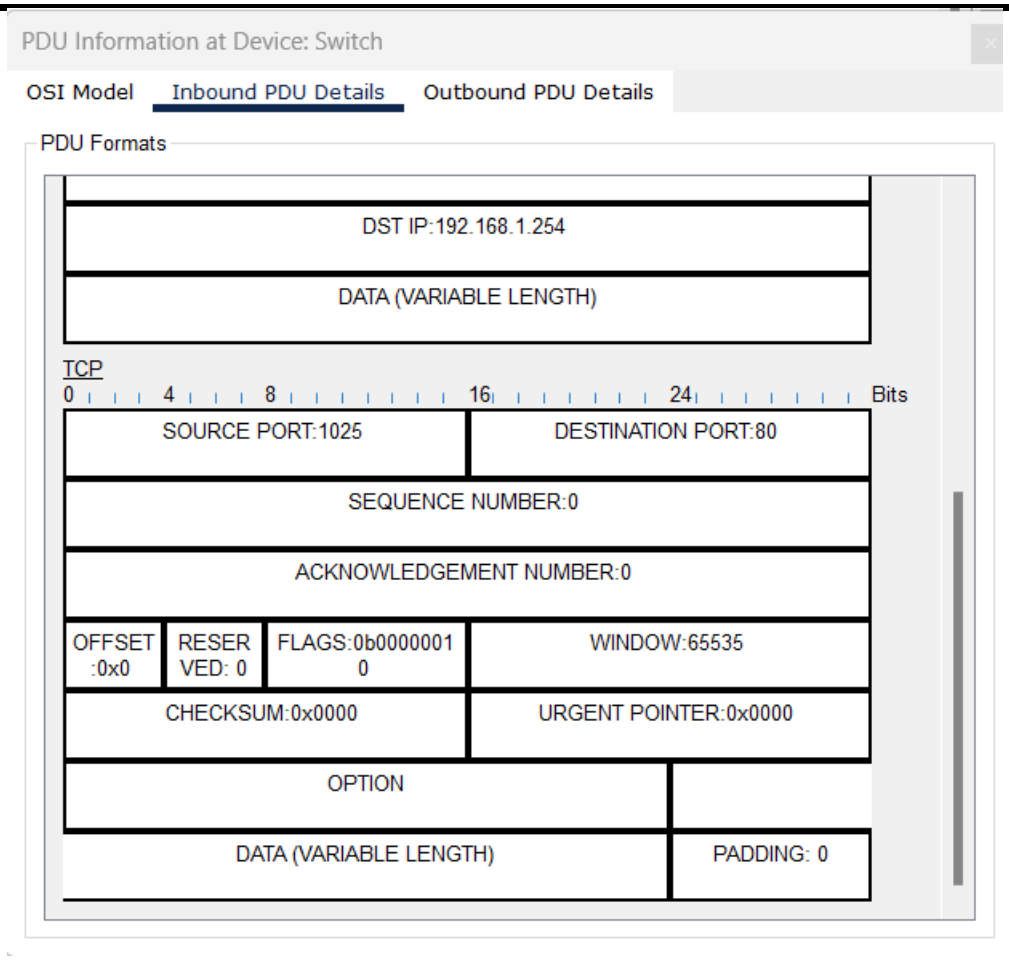
b. Click **Capture/Forward**. Hold your mouse above each PDU until you find one that originates from **HTTP Client**. Click the PDU envelope to open it.



c. Click the **Inbound PDU Details** tab and scroll down to the last section. What is the section labeled?

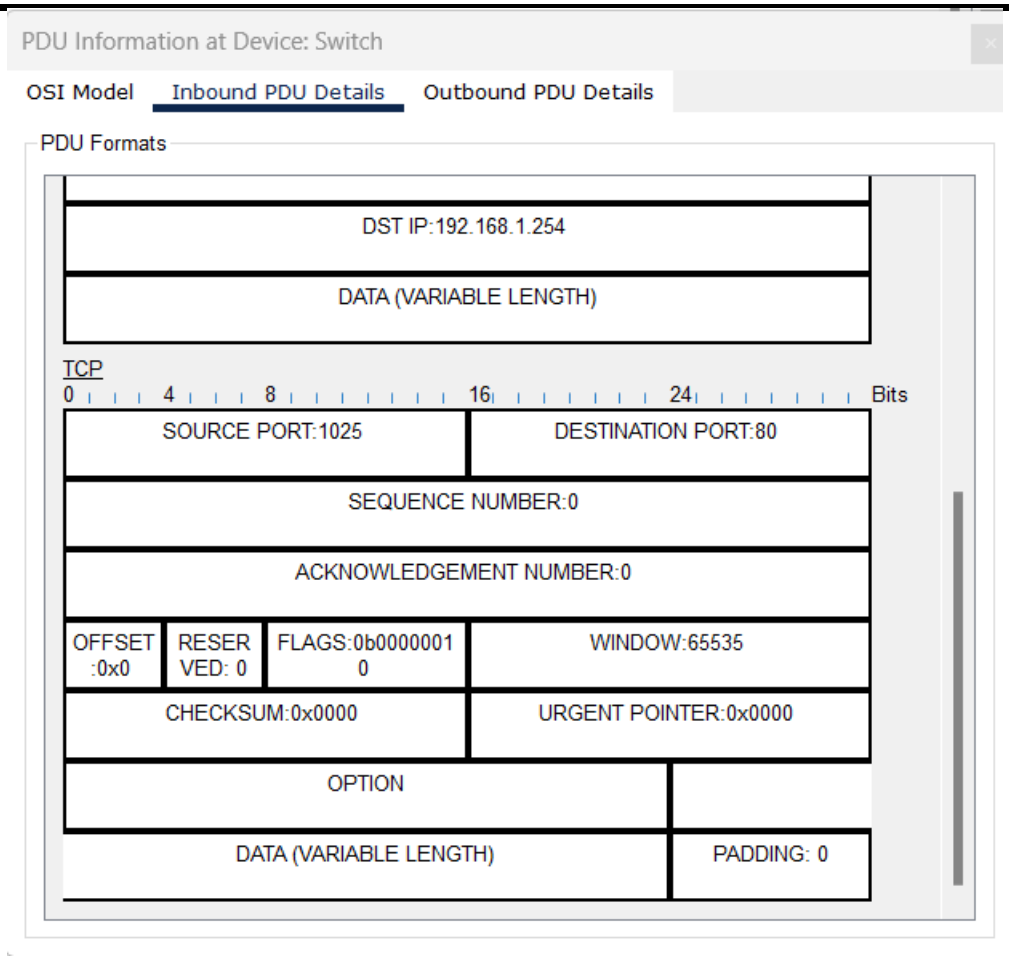
Are these communications considered to be reliable?

TCP is labeled in the last section.
Yes. TCP is a reliable transport protocol which has a connection-oriented communication between the sending and receiving process.

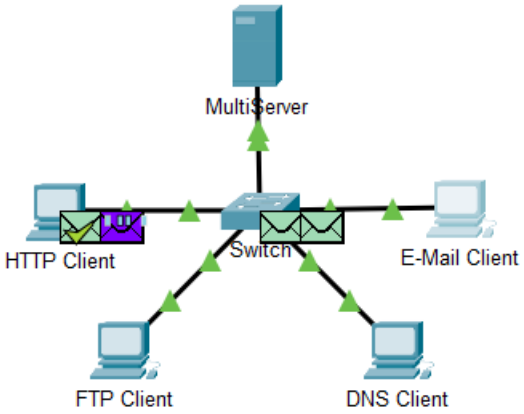


d. Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values. What is written in the field to the left of the **WINDOW** field?

SRC PORT=1025, DEST PORT=80, SEQUENCE NUM=0, ACK NUM=0, FLAGS=SYN



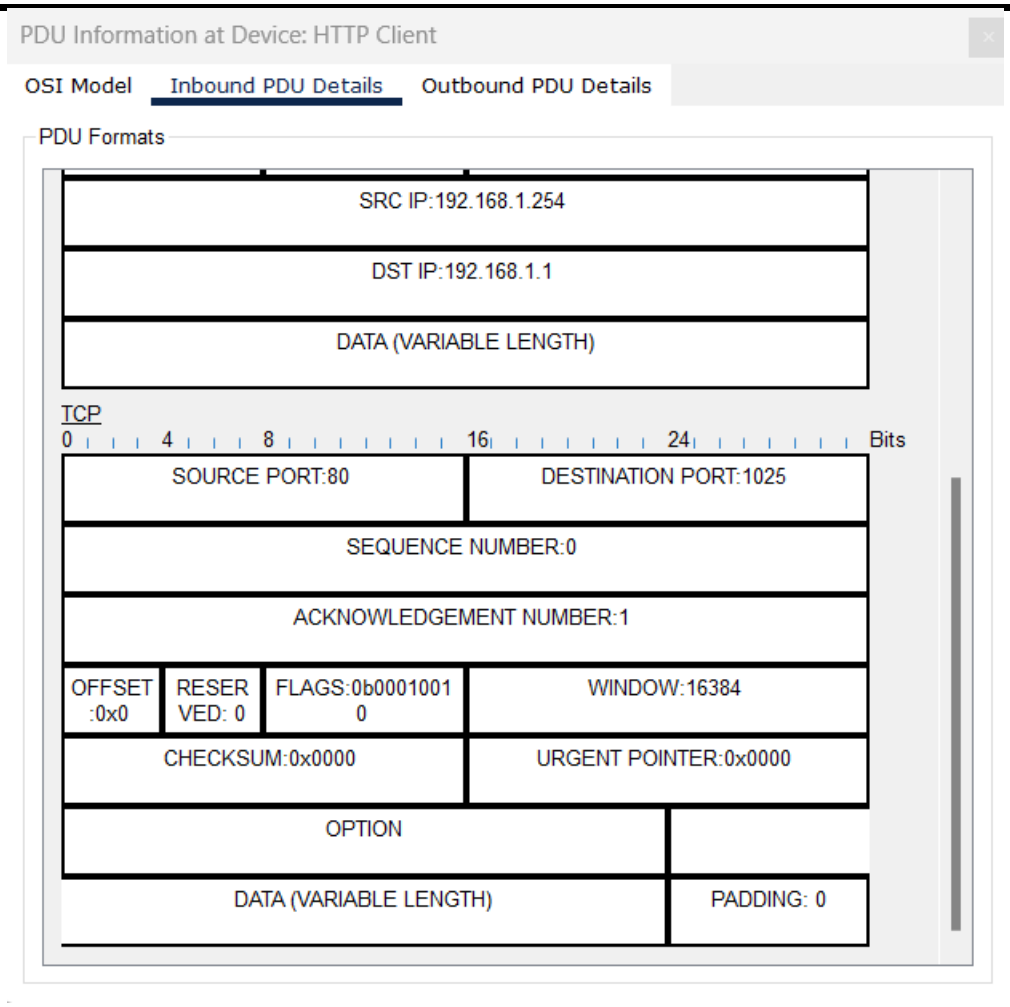
e. Close the PDU and click **Capture/Forward** until a PDU returns to the **HTTP Client** with a checkmark.



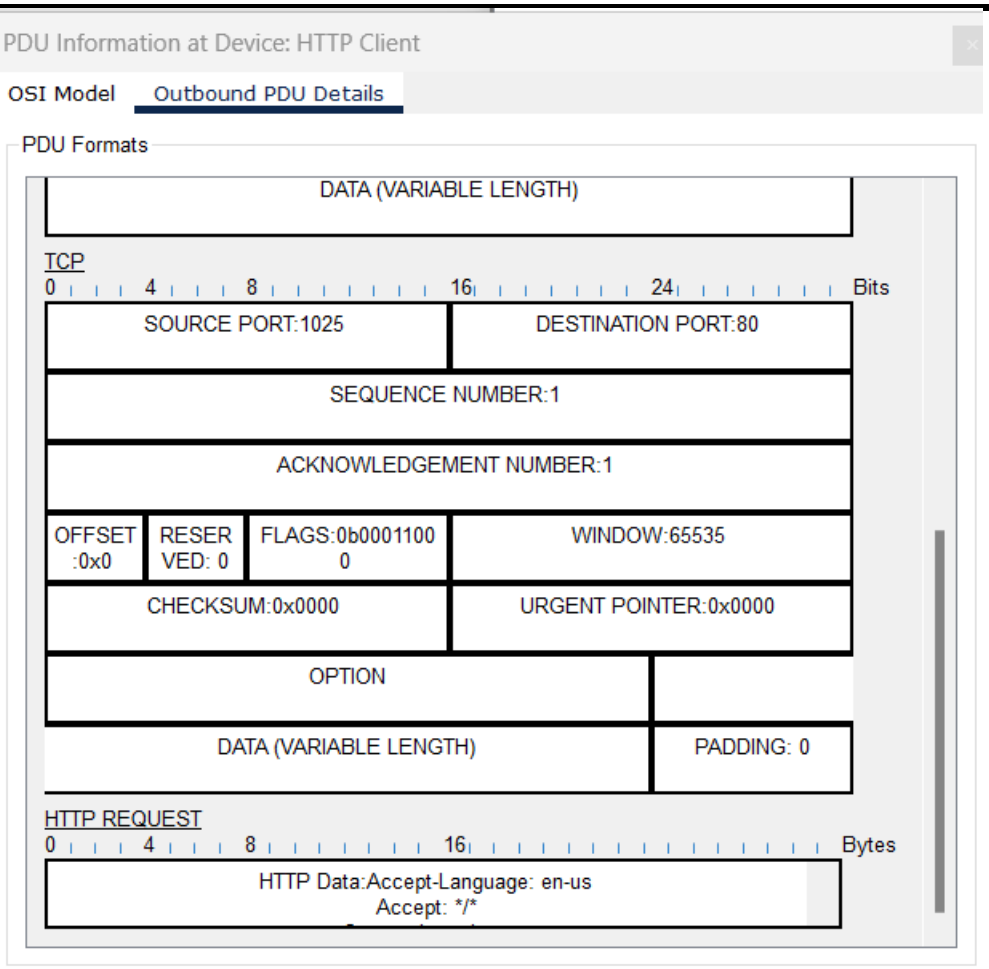
f. Click the PDU envelope and select **Inbound PDU Details**. How are the port and sequence numbers different than before?

SRC PORT=80 (reversed), DEST PORT=1025 (reversed), SEQUENCE NUM=0 (Unchanged), ACK NUM=1 (Changed), FLAGS=SYN+ACK (FLAGS changed to SYN+ACK)

SRS PORT and DEST PORT are reversed, ACK NUM changed to 1, and FLAGS changed to SYN+ACK.



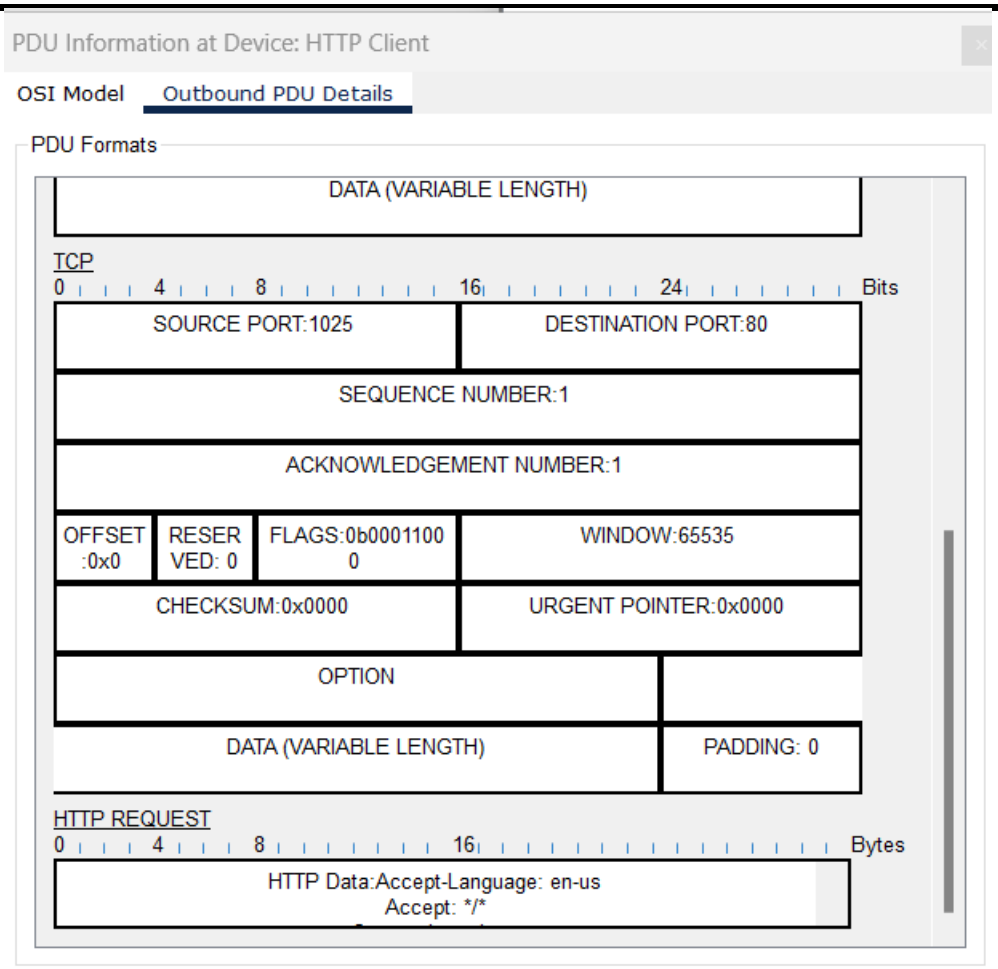
g. There is a second **PDU** of a different color, which **HTTP Client** has prepared to send to **MultiServer**. This is the beginning of the HTTP communication. Click this second PDU envelope and select **Outbound PDU Details**.



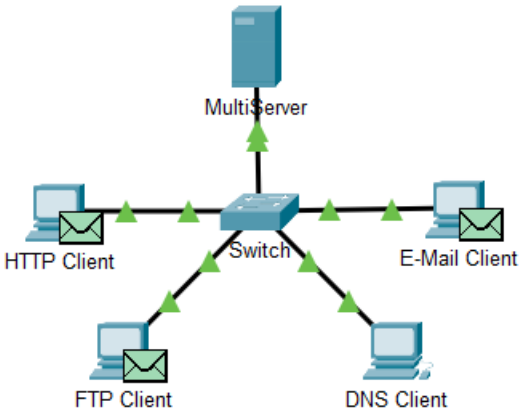
h. What information is now listed in the TCP section? How are the port and sequence numbers different from the previous two PDUs?

SRC PORT=1025 (same as first PDU), DEST PORT=80 (same with first PDU), SEQUENCE NUM=1 (Changed), ACK NUM=1 (Unchanged), FLAGS=PSH+ACK (FLAGS changed to PSH+ACK)

SRS PORT and DEST PORT are reversed, SEQUENCE NUM and ACK NUM changed to 1, and FLAGS changed to PSH+ACK.

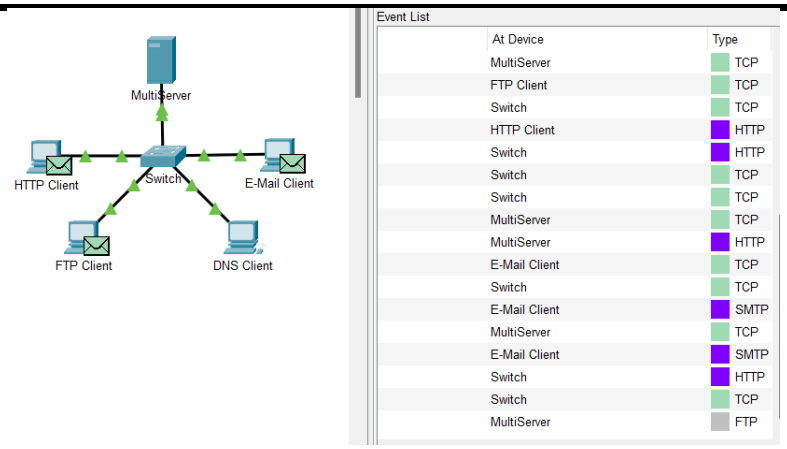


i. Click **Back** until the simulation is reset.

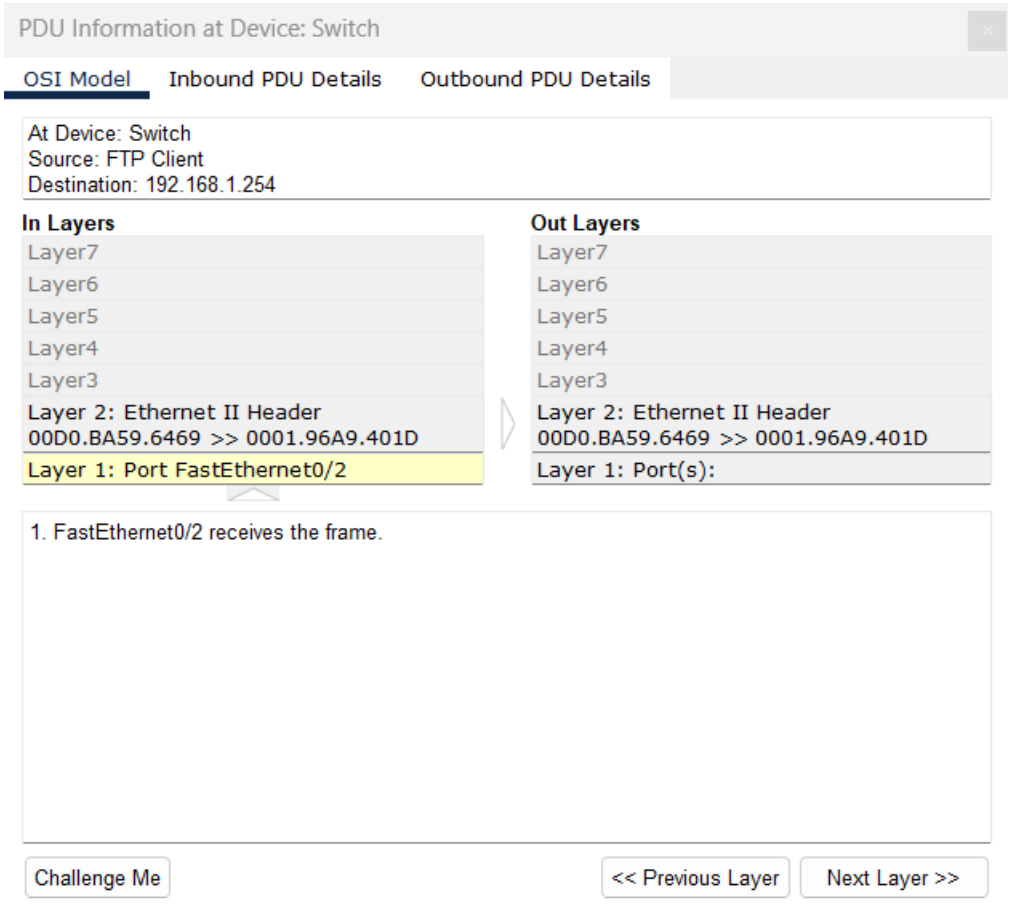


Step 3: Examine FTP traffic as the clients communicate with the server.

a. In the Simulation Panel, change **Edit Filters** to display only **FTP** and **TCP**.



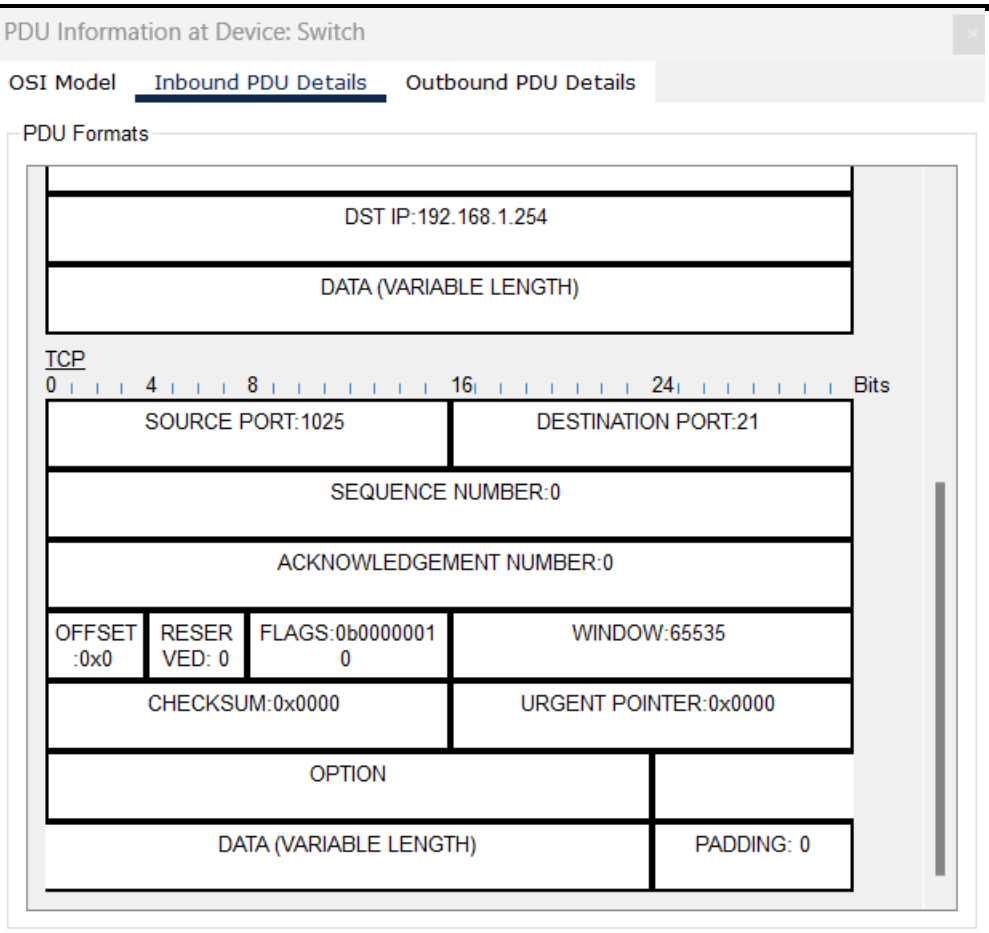
b. Click **Capture/Forward**. Hold your cursor above each PDU until you find one that originates from **FTP Client**. Click that PDU envelope to open it.



c. Click the **Inbound PDU Details** tab and scroll down to the last section. What is the section labeled?

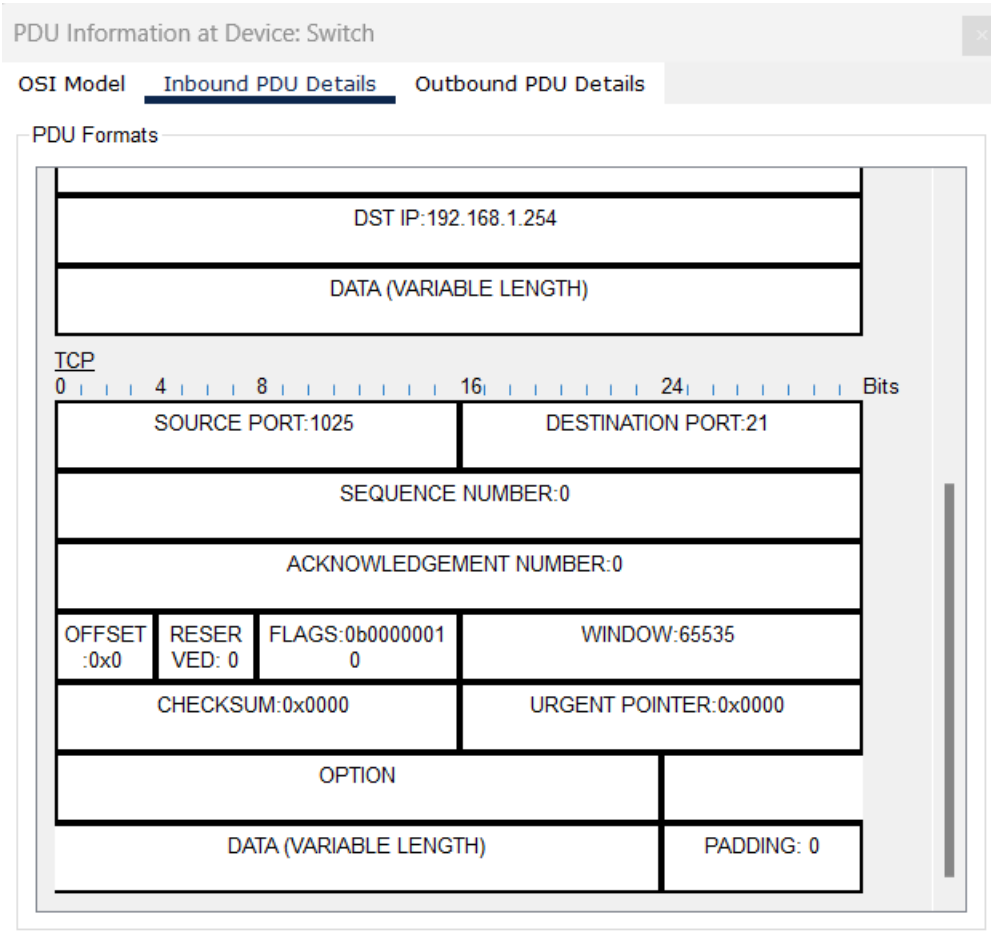
Are these communications considered to be reliable?

The last section labeled is TCP.
Yes. TCP is a reliable transport protocol which has a connection-oriented communication between the sending and receiving process.

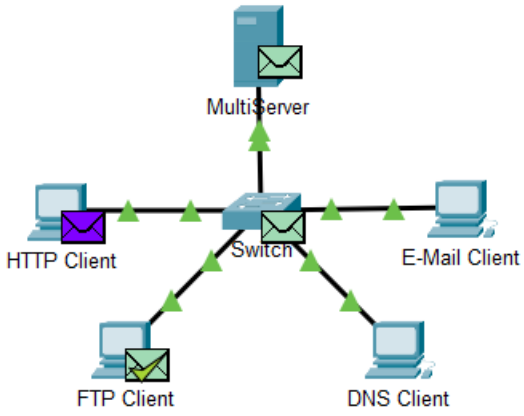


d. Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values. What is written in the field to the left of the **WINDOW** field?

SRC PORT=1025, DEST PORT=21, SEQUENCE NUM=0, ACK NUM=0, FLAGS=SYN



e. Close the PDU and click **Capture/Forward** until a PDU returns to the **FTP Client** with a checkmark.

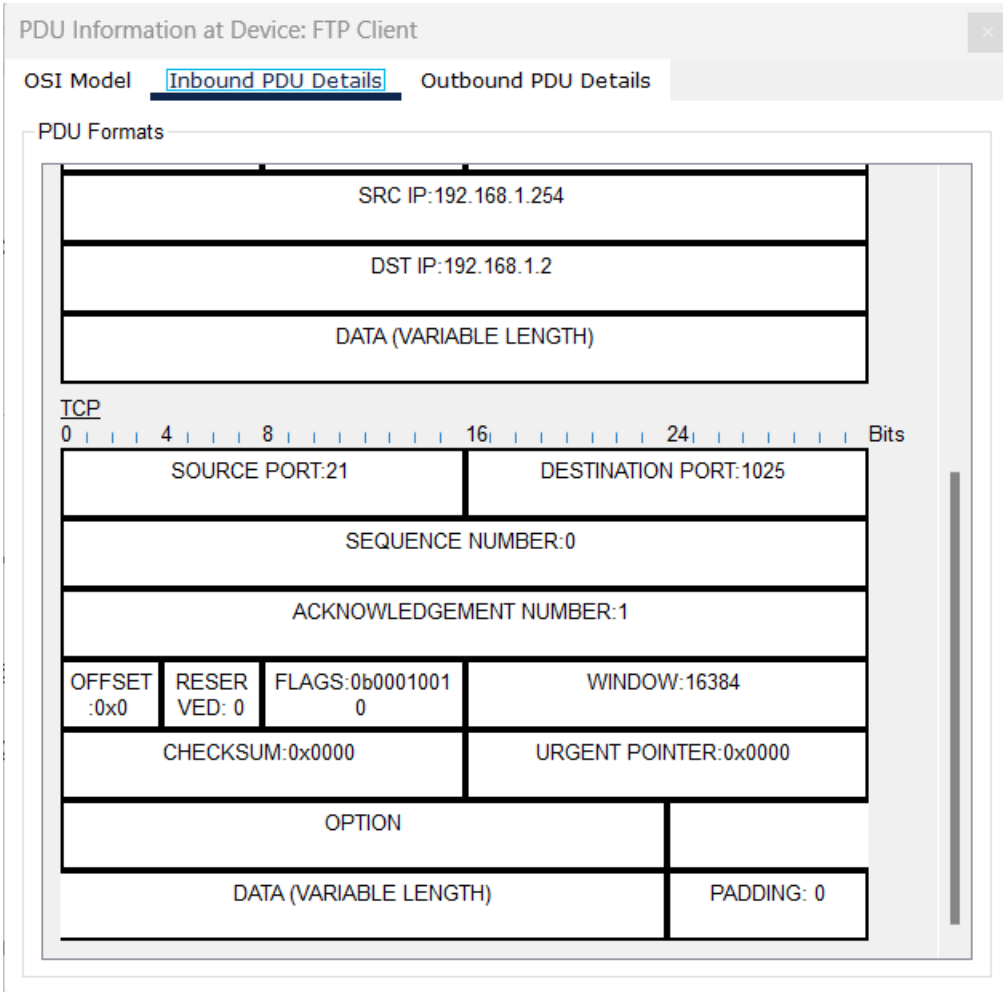


f. Click the PDU envelope and select **Inbound PDU Details**. How are the port and sequence numbers

different than before?

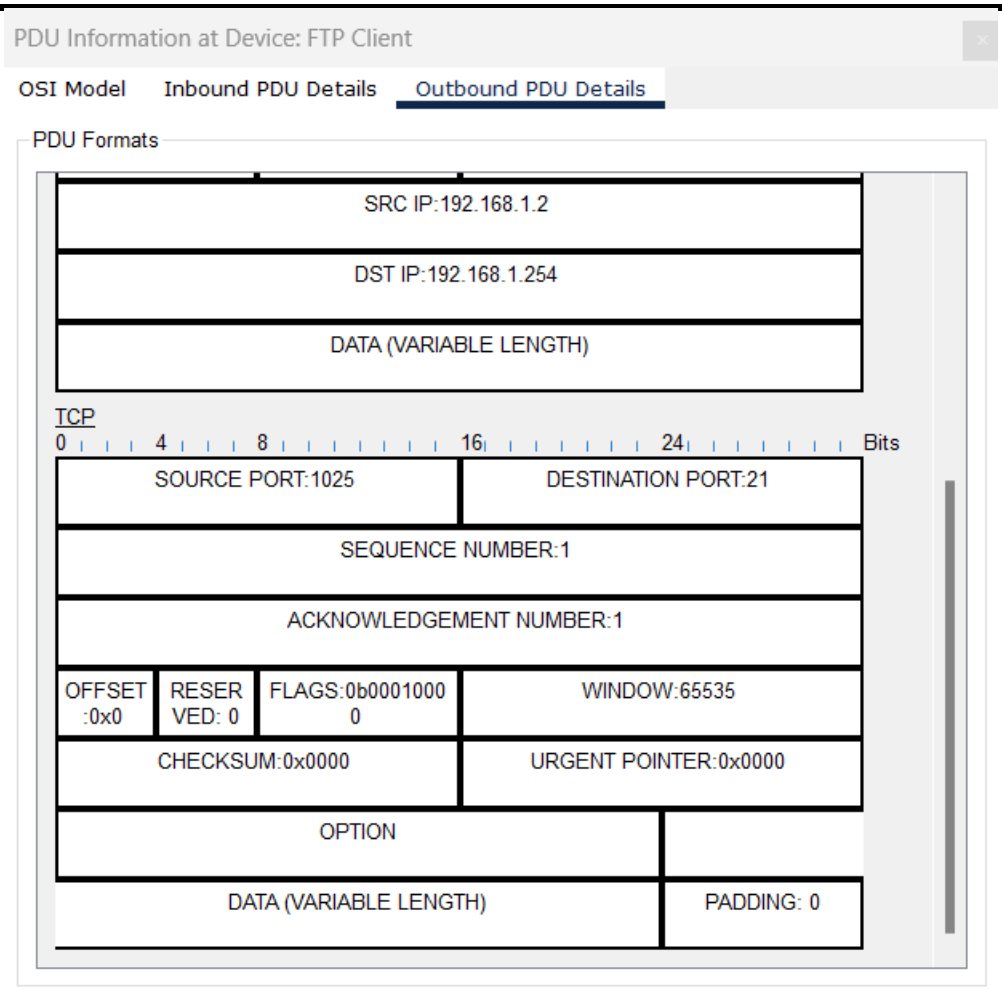
SRC PORT=21 (reversed), DEST PORT=1025 (reversed), SEQUENCE NUM=0 (Unchanged), ACK NUM=1 (Changed), FLAGS=SYN+ACK (FLAGS changed to SYN+ACK)

SRS PORT and DEST PORT are reversed, ACK NUM changed to 1, and FLAGS changed to SYN+ACK.

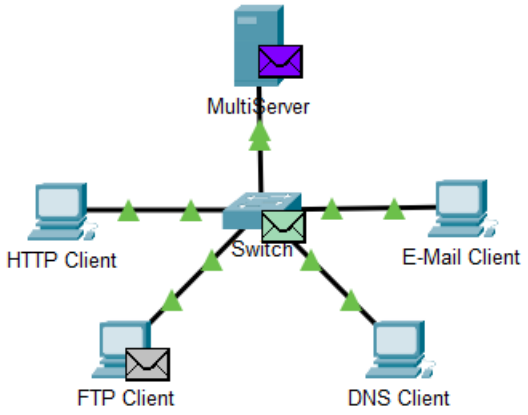


g. Click the **Outbound PDU Details** tab. How are the port and sequence numbers different from the previous two results?

SRC PORT=1025 (same as first PDU), DEST PORT=21 (same as first PDU), SEQUENCE NUM=1 (Changed), ACK NUM=1 (Unhanged), FLAGS=ACK (FLAGS changed to ACK)
SRC PORT and DEST PORT are reversed, SEQUENCE NUM and ACK NUM changed to 1, and FLAGS changed to ACK

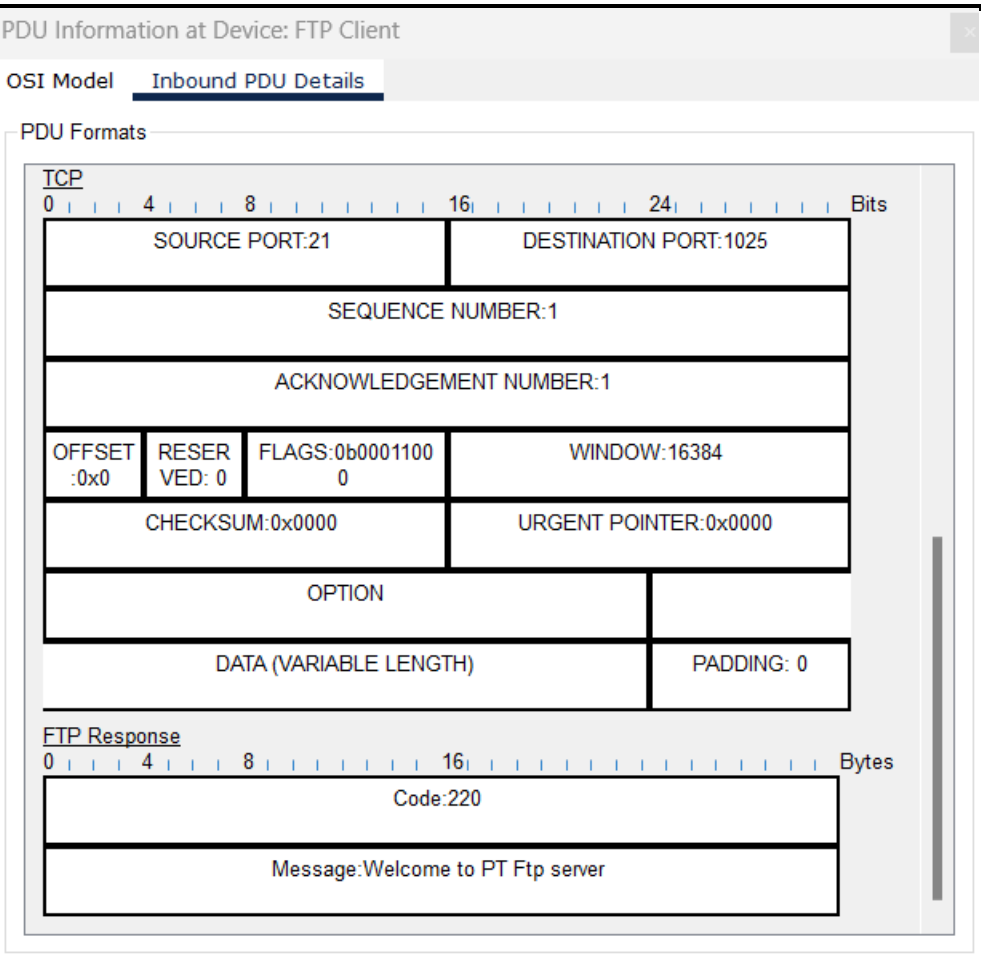


h. Close the PDU and click **Capture/Forward** until a second PDU returns to the **FTP Client**. The PDU is a different color.

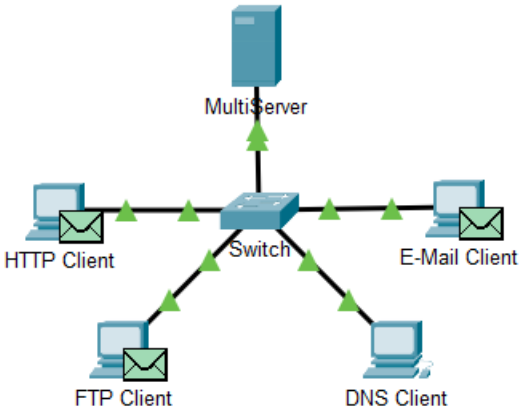


i. Open the PDU and select **Inbound PDU Details**. Scroll down past the TCP section. What is the message from the server?

Message from the server: "Welcome to PT Ftp server"

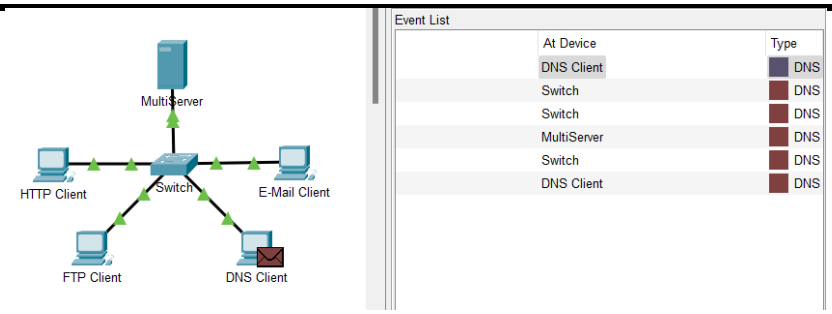


j. Click **Back** until the simulation is reset.

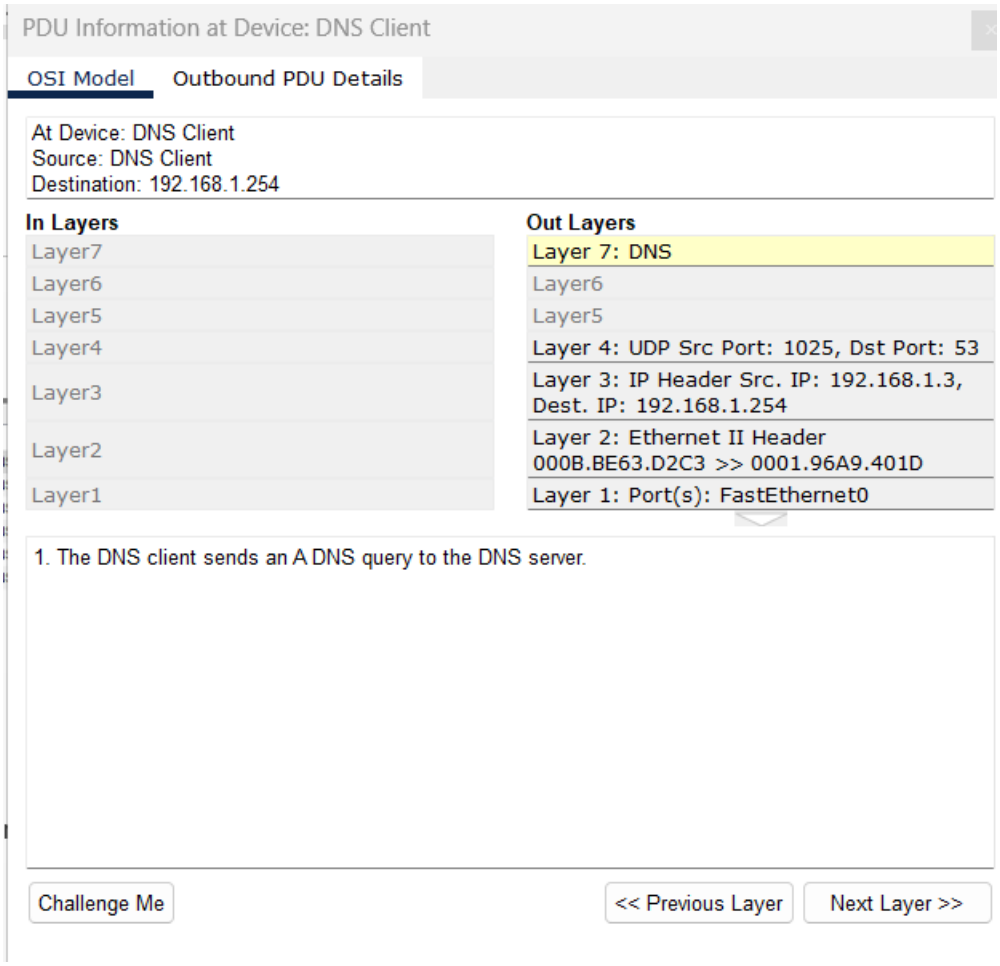


Step 4: Examine DNS traffic as the clients communicate with the server.

a. In the Simulation Panel, change **Edit Filters** to display only **DNS** and **UDP**.



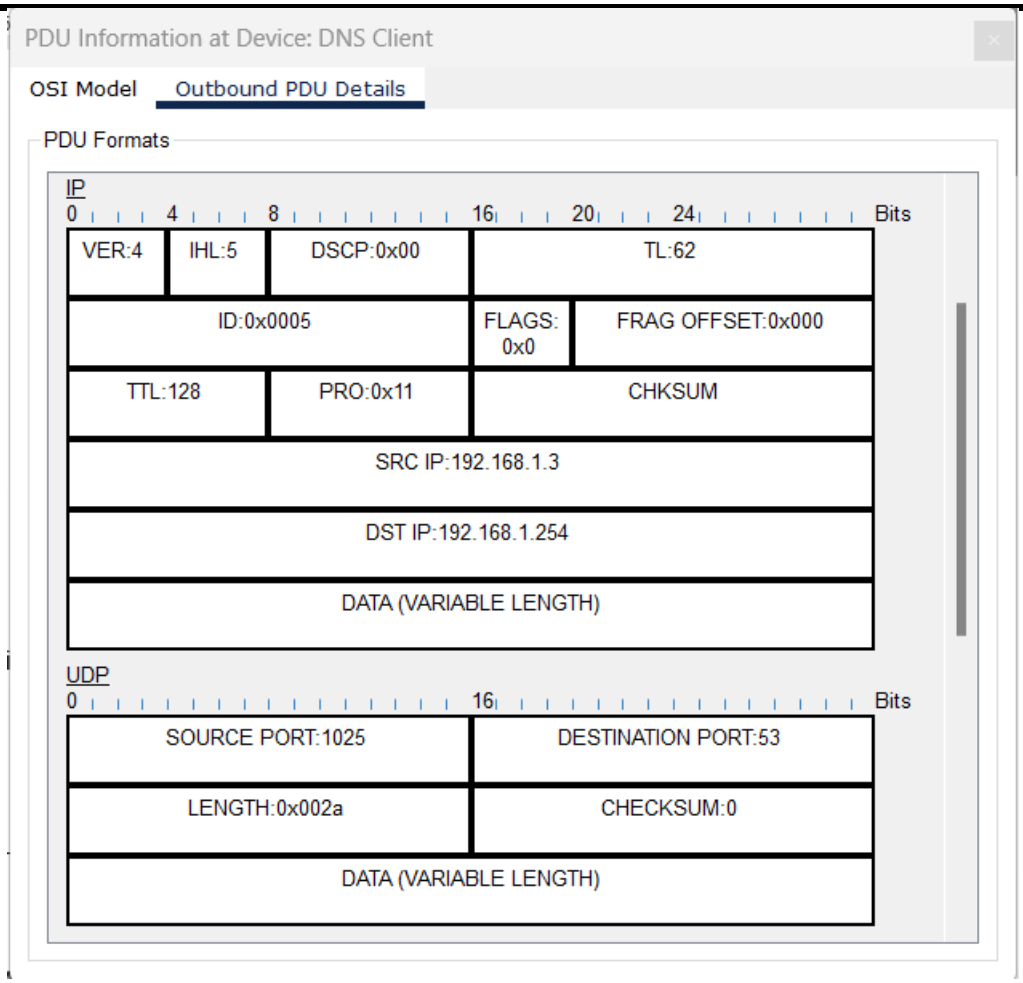
b. Click the PDU envelope to open it.



c. Click the **Inbound PDU Details** tab and scroll down to the last section. What is the section labeled?

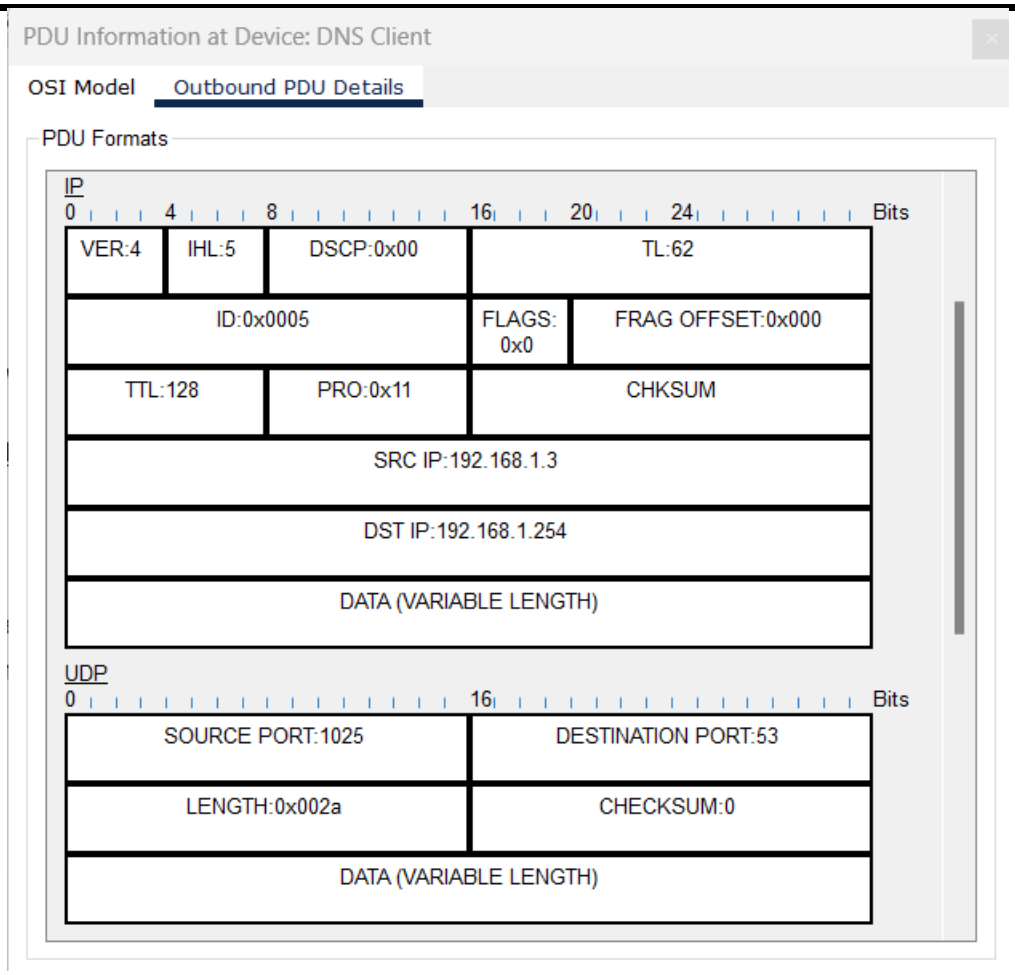
Are these communications considered to be reliable?

The last section labeled is UDP.
No. UDP is unreliable transport protocol between sending and receiving process because it does not have a connection-oriented communication.

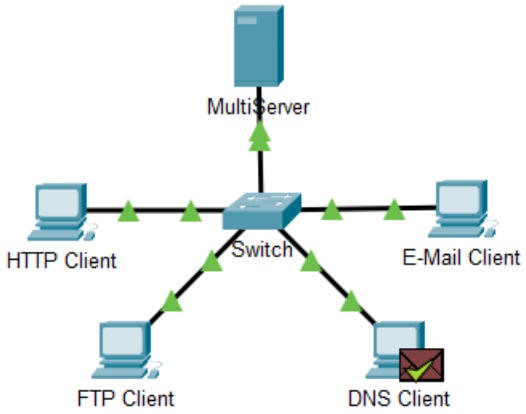


d. Record the **SRC PORT** and **DEST PORT** values. Why is there no sequence and acknowledgement number?

SRC PORT=1025, DEST PORT=53. There is no sequence and acknowledgement number because UDP need not establish a reliable connection.



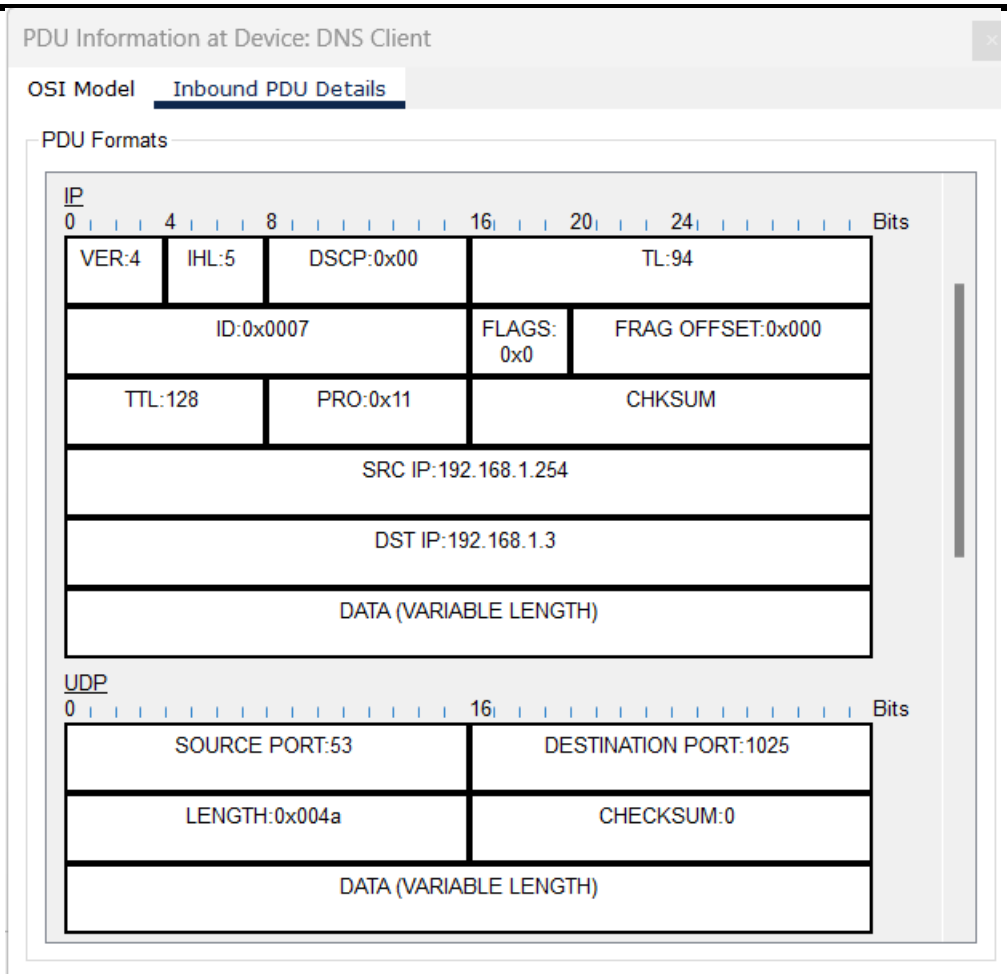
e. Close the **PDU** and click **Capture/Forward** until a PDU returns to the **DNS Client** with a checkmark.



f. Click the PDU envelope and select **Inbound PDU Details**. How are the port and sequence numbers different than before?

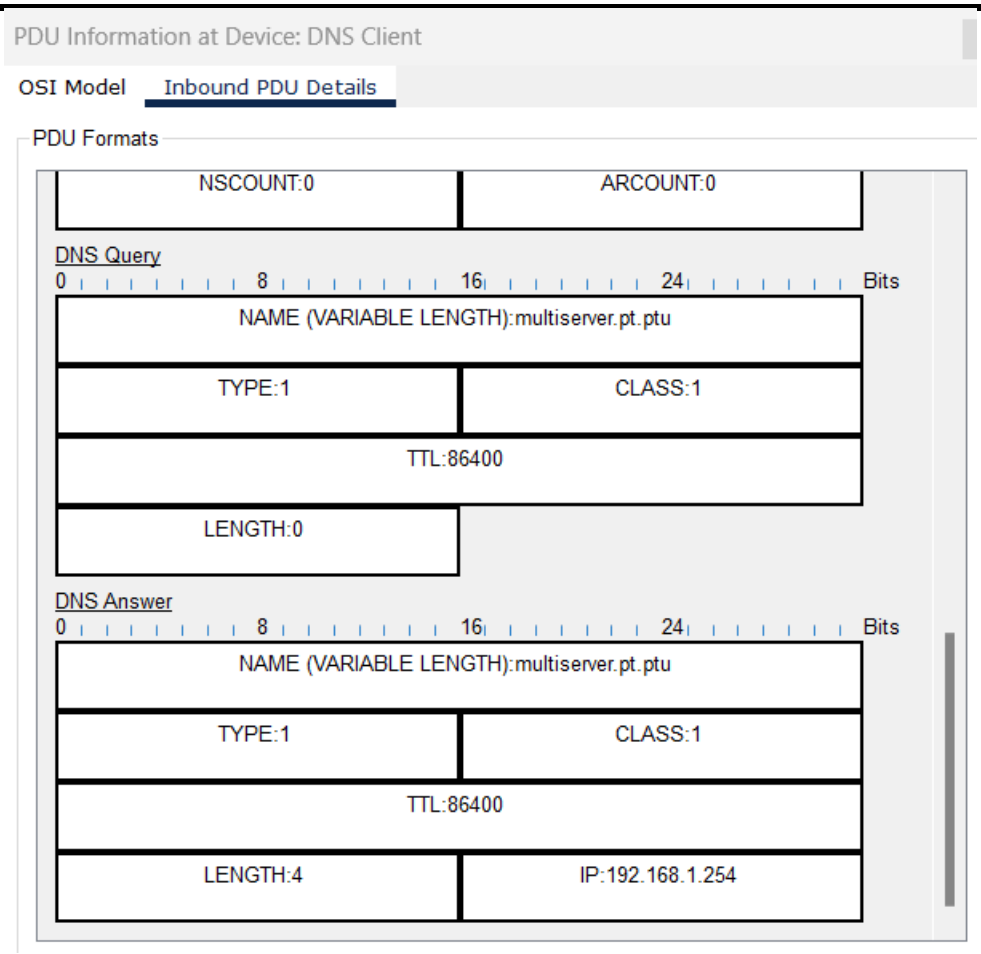
SRC PORT=53 (reversed), DEST PORT=1025 (reversed)

SRC PORT and DEST PORT are reversed. No SEQUENCE NUM and ACK NUM found in UDP.

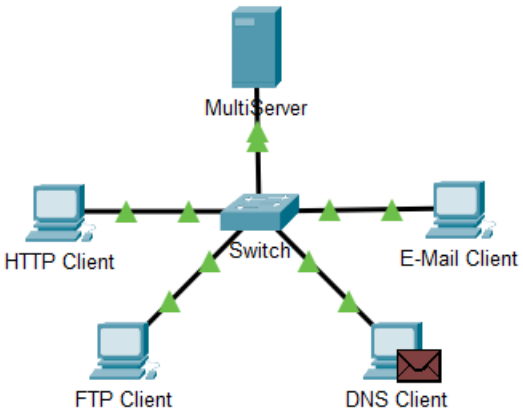


g. What is the last section of the **PDU** called?

DNS Answer

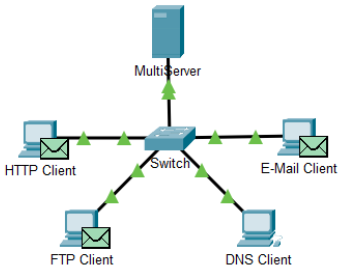


h. Click **Back** until the simulation is reset.



Step 5: Examine email traffic as the clients communicate with the server.

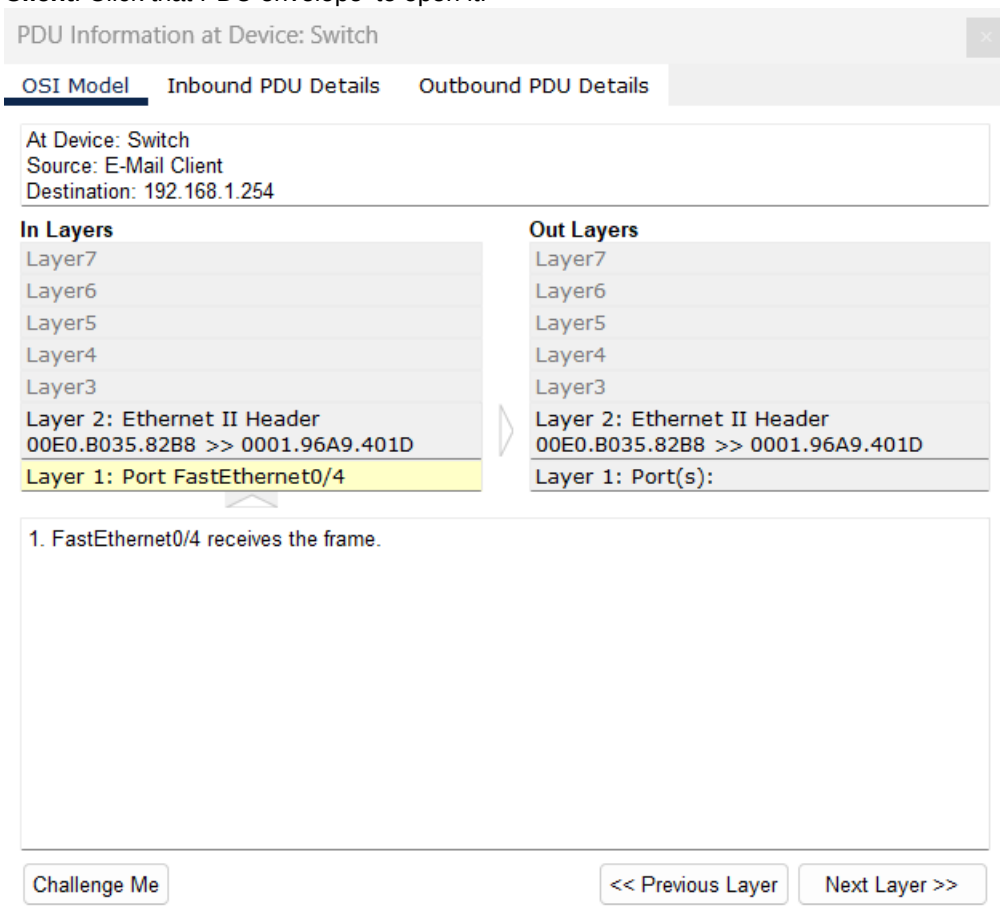
a. In the Simulation Panel, change **Edit Filters** to display only **POP3, SMTP** and **TCP**.



Event List

	At Device	Type
	MultiServer	HTTP
	E-Mail Client	TCP
	Switch	TCP
	E-Mail Client	SMTP
	MultiServer	TCP
	E-Mail Client	SMTP
	Switch	HTTP
	Switch	TCP
	MultiServer	FTP
	Switch	SMTP
	Switch	FTP
	HTTP Client	HTTP
	MultiServer	TCP
	HTTP Client	TCP
	MultiServer	SMTP
	FTP Client	FTP
	Switch	TCP

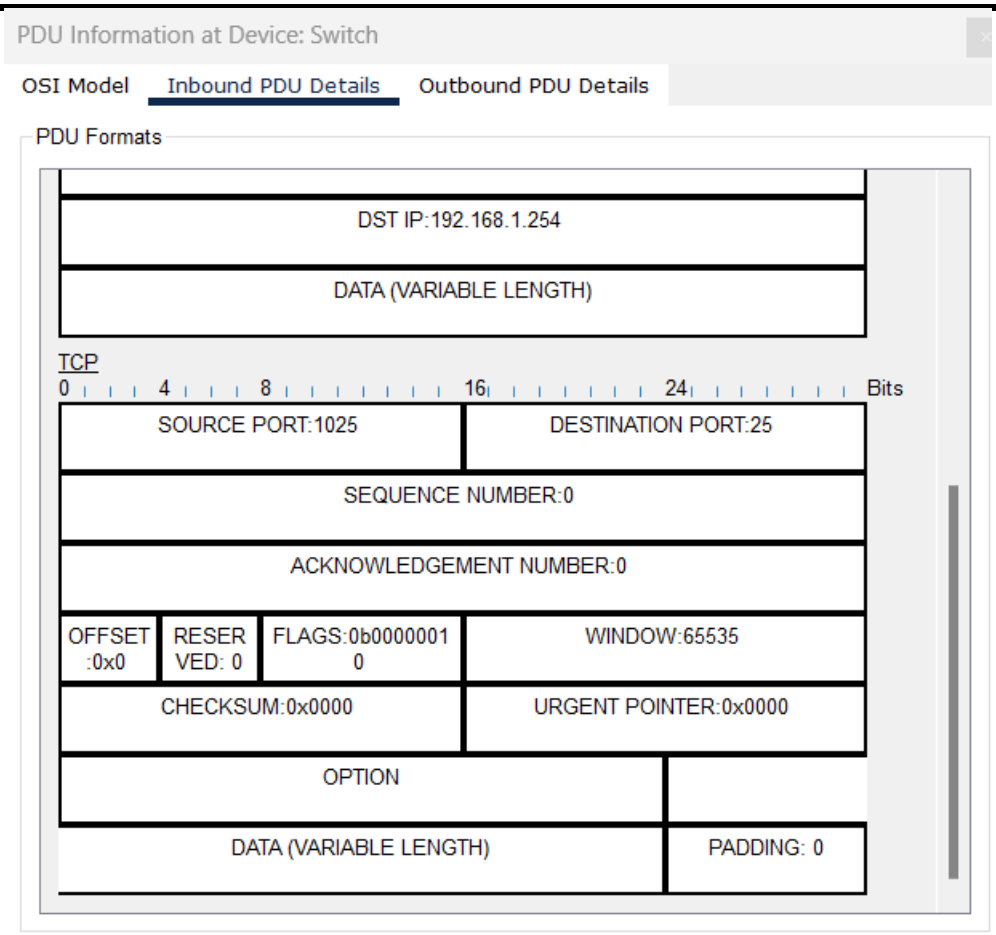
b. Click **Capture/Forward**. Hold your cursor above each PDU until you find one that originates from **E-mail Client**. Click that PDU envelope to open it.



c. Click the **Inbound PDU Details** tab and scroll down to the last section. What transport layer protocol does email traffic use?

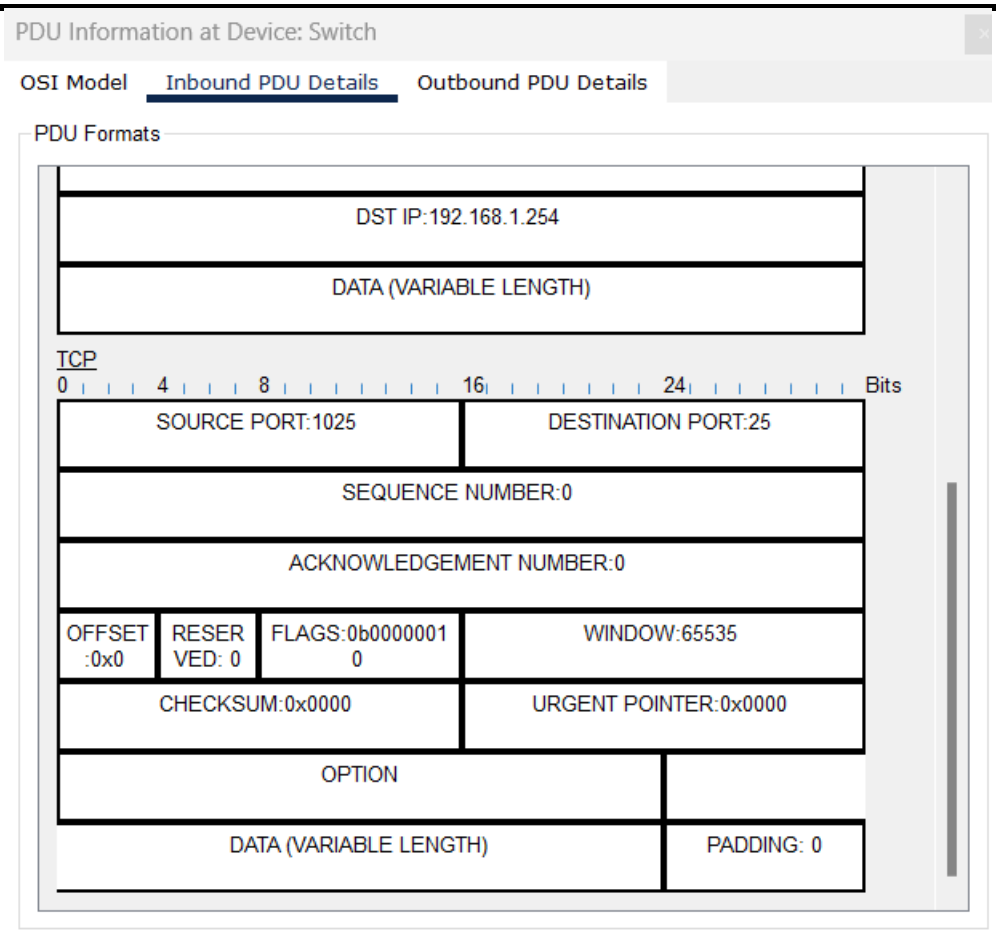
Are these communications considered to be reliable?

The last section labeled is TCP.
Yes. TCP is a reliable transport protocol which has a connection-oriented communication between the sending and receiving process.

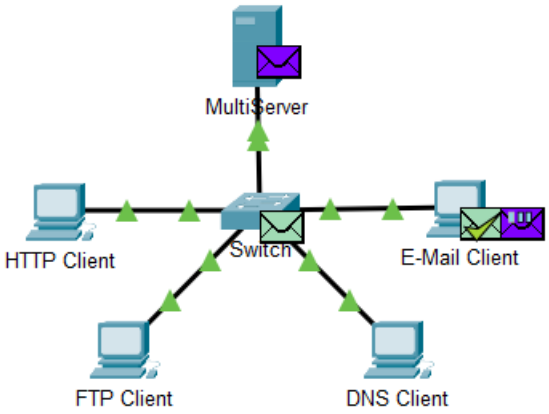


d. Record the **SRC PORT**, **DEST PORT**, **SEQUENCE NUM**, and **ACK NUM** values. What is written in the field to the left of the **WINDOW** field?

SRC PORT=1025, DEST PORT=25, SEQUENCE NUM=0, ACK NUM=0, FLAGS=SYN

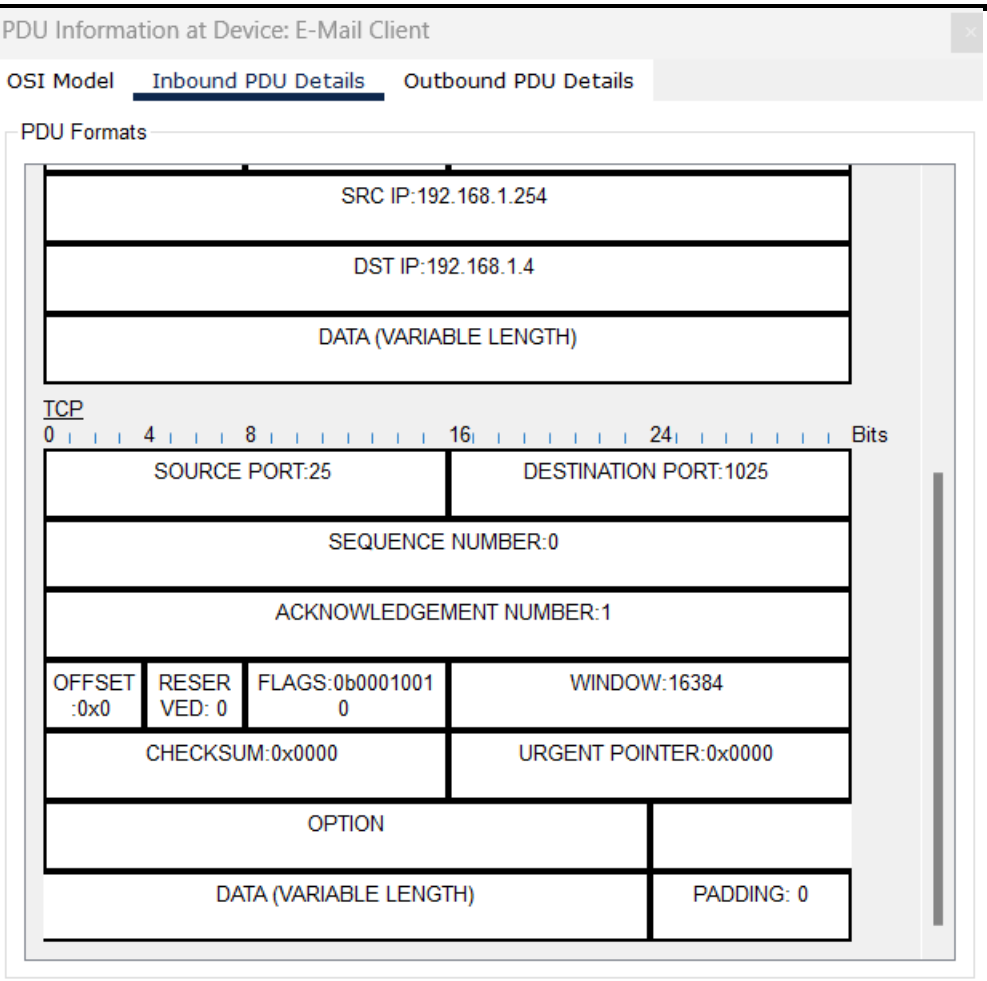


e. Close the **PDU** and click **Capture/Forward** until a PDU returns to the **E-Mail Client** with a checkmark.



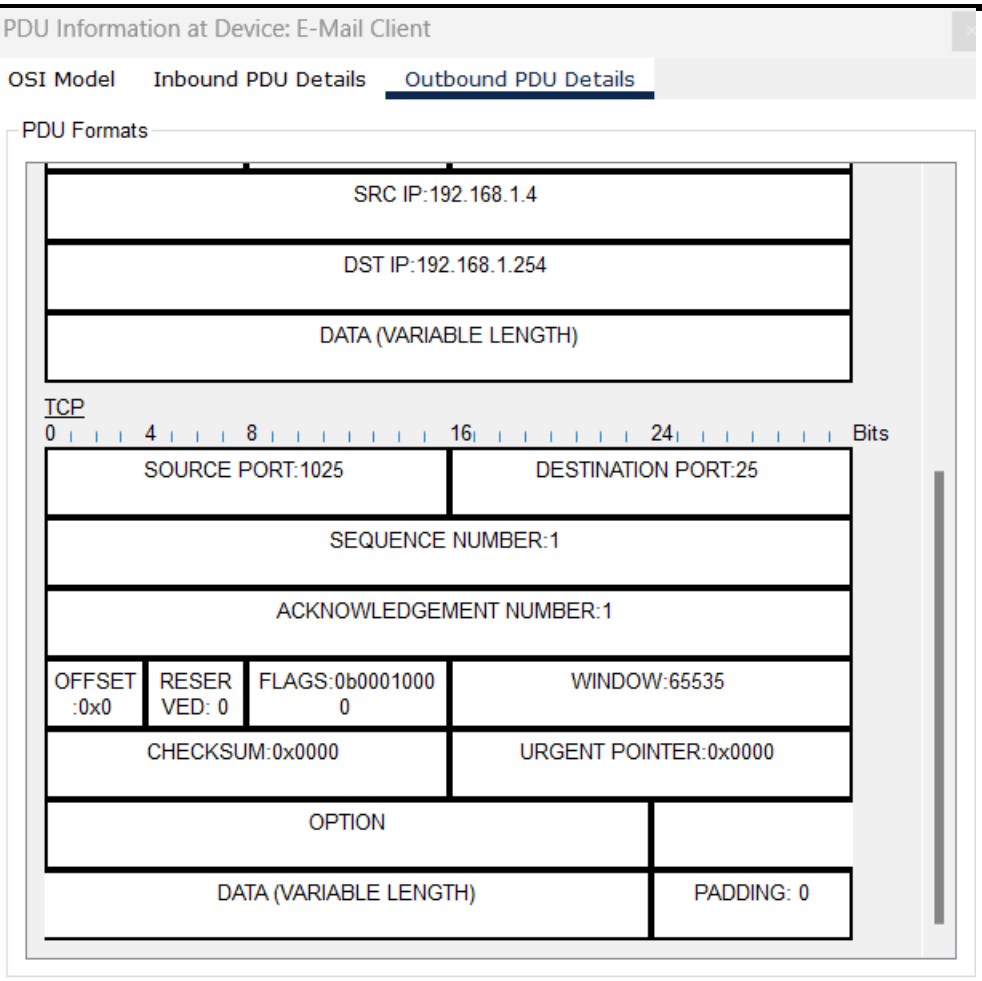
f. Click the PDU envelope and select **Inbound PDU Details**. How are the port and sequence numbers different than before?

SRC PORT=25 (reversed), DEST PORT=1025 (reversed), SEQUENCE NUM=0 (Unchanged), ACK NUM=1 (Changed), FLAGS=SYN+ACK (FLAGS changed to SYN+ACK)
SRC PORT and DEST PORT are reversed, ACK NUM changed to 1, and FLAGS changed to SYN + ACK

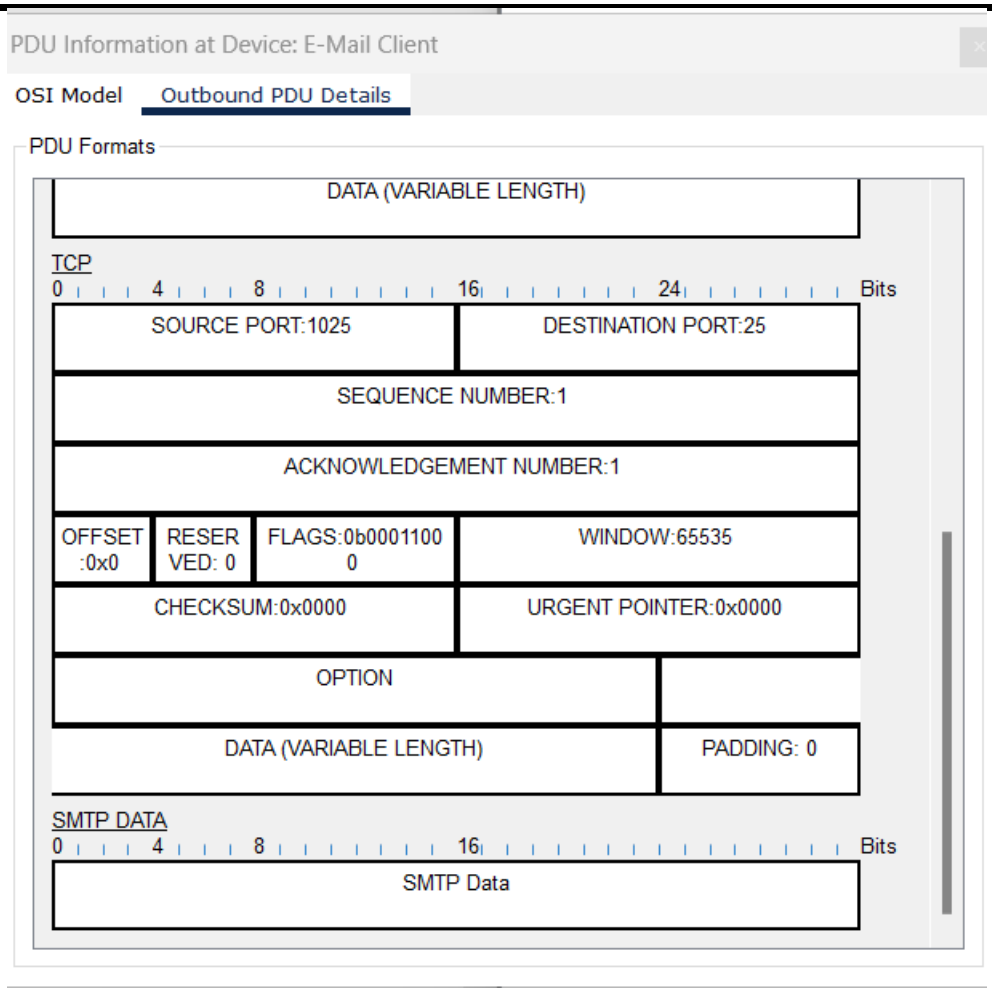


g. Click the **Outbound PDU Details** tab. How are the port and sequence numbers different from the previous two results?

SRC PORT=1025 (same as first PDU), DEST PORT=25 (same as first PDU), SEQUENCE NUM=1 (Changed), ACK NUM=1 (Unhanged), FLAGS=ACK (FLAGS changed to ACK)
SRC PORT and DEST PORT are reversed, SEQUENCE NUM and ACK NUM changed to 1, and FLAGS changed to ACK

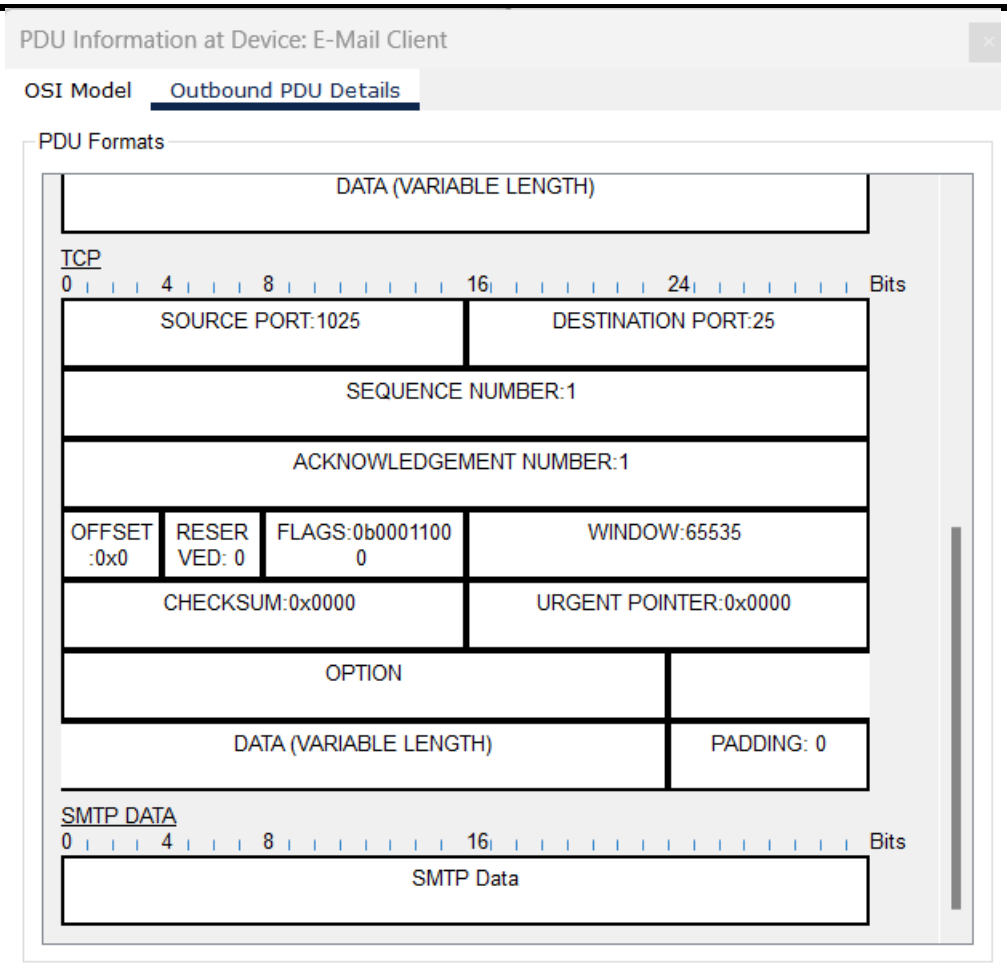


h. There is a second **PDU** of a different color that **HTTP Client** has prepared to send to **MultiServer**. This is the beginning of the email communication. Click this second PDU envelope and select **Outbound PDU Details.**



i. How are the port and sequence numbers different from the previous two **PDU**s?

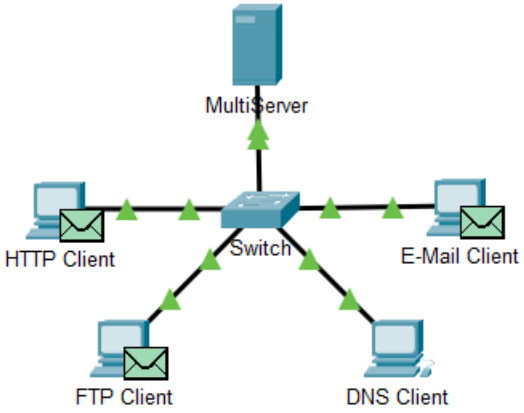
SRC PORT=1025 (same as first PDU), DEST PORT=25 (same as first PDU), SEQUENCE NUM=1 (Changed), ACK NUM=1 (Unhanged), FLAGS=PSH+ACK (FLAGS changed to PSH+ACK)
SRC PORT and DEST PORT are reversed, SEQUENCE NUM and ACK NUM changed to 1, and FLAGS changed to PSH+ACK



j. What email protocol is associated with TCP port 25? What protocol is associated with TCP port 110?

SMTP is associated with TCP port 25, whereas POP3 is associated with TCP port 110.

k. Click **Back** until the simulation is reset.



Step 6: Examine the use of port numbers from the server.

a. To see TCP active sessions, perform the following steps in quick succession:

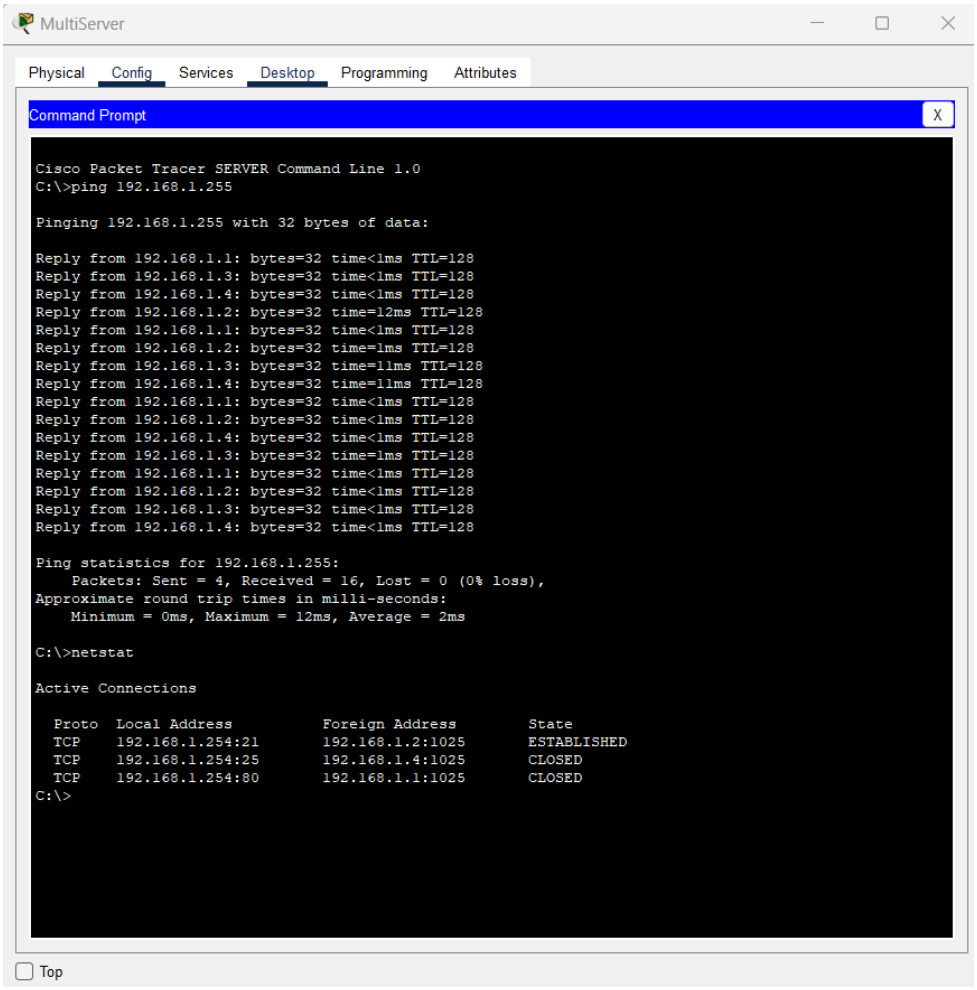
1) Switch back to **Realtime** mode.

2) Click **MultiServer** and click the **Desktop** tab > **Command Prompt**.

b. Enter the **netstat** command. What protocols are listed in the left column?

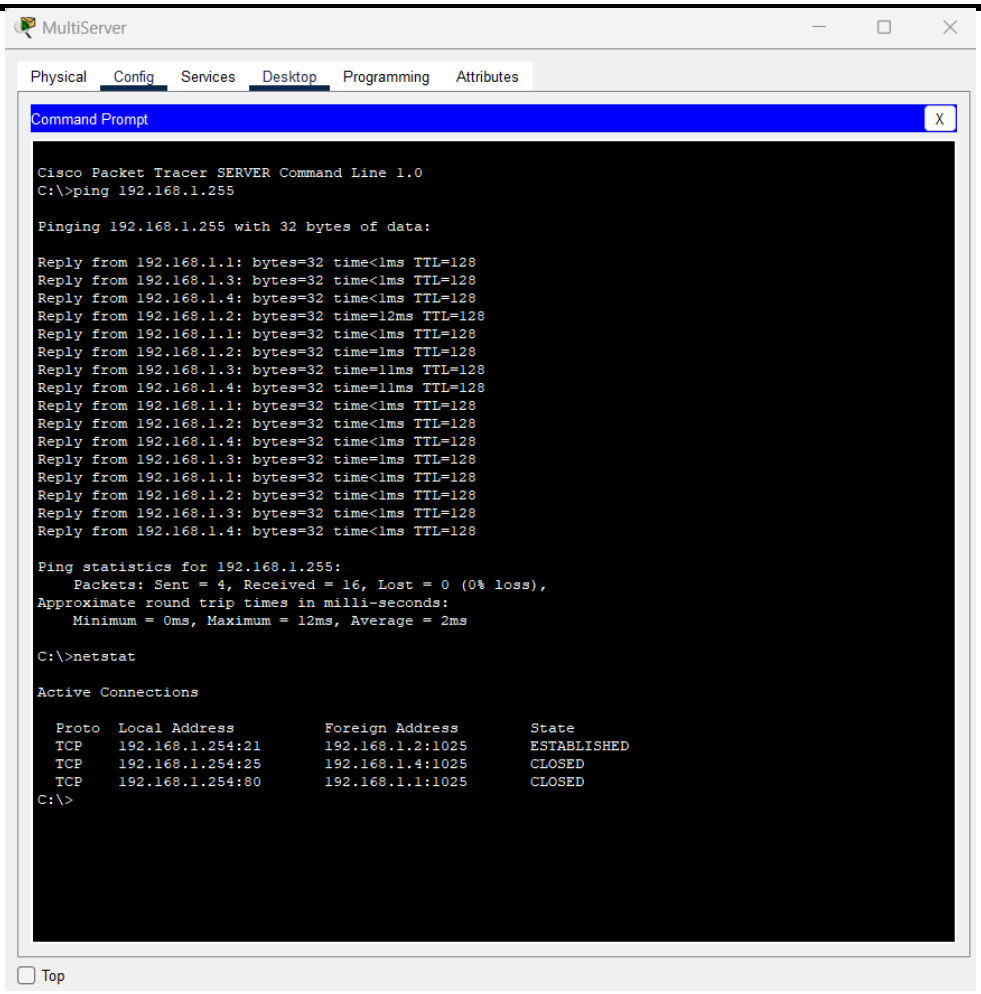
What port numbers are being used by the server?

TCP. Port numbers: 21, 25, 80



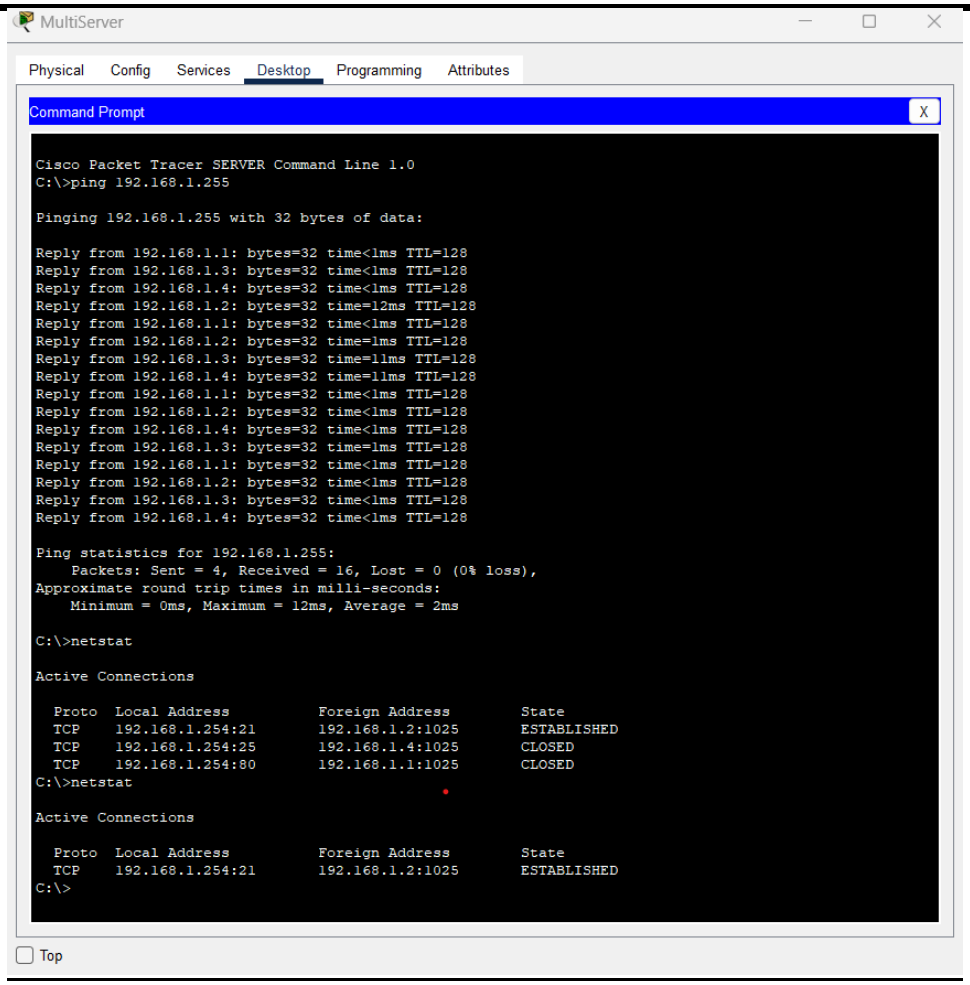
c. What states are the sessions in?

ESTABLISHED, CLOSED



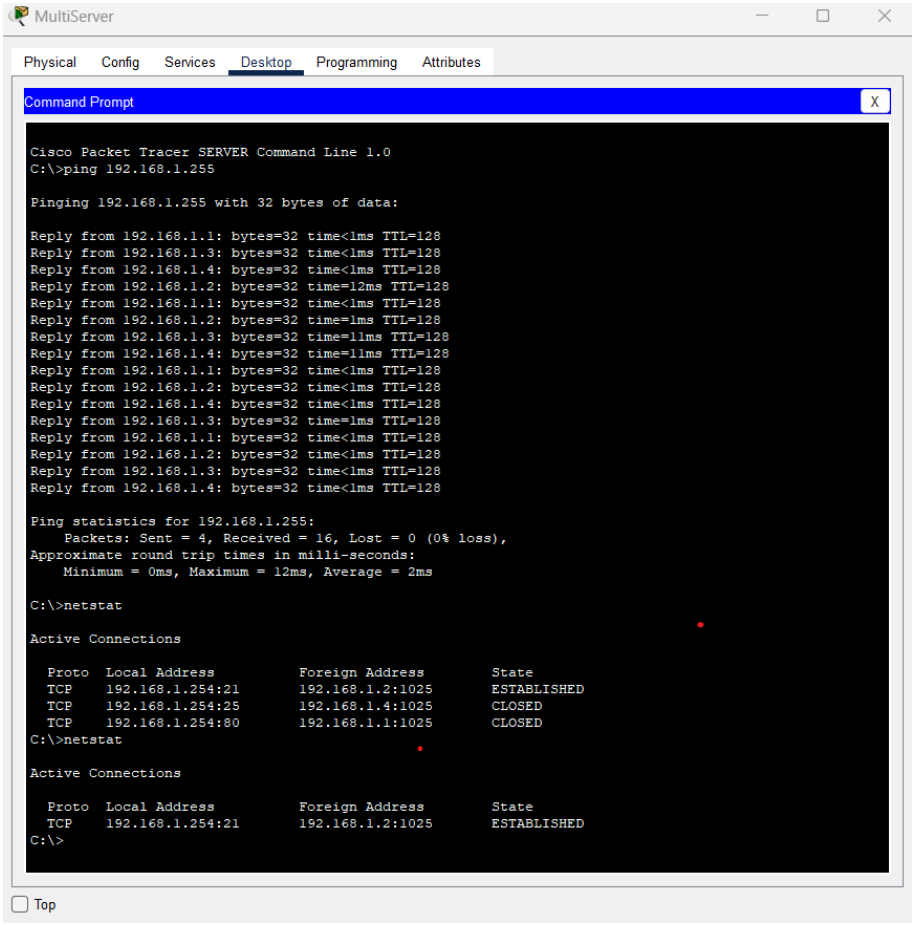
d. Repeat the **netstat** command several times until you see only one session still ESTABLISHED. For which service is this connection still open?

FTP



Why doesn't this session close like the other three? (Hint: Check the minimized clients)

The server is waiting for the user input.



Suggested Scoring Rubric

Activity Section	Question Location	Possible Points	Earned Points
Part 2: Examine Functionality of the TCP and UDP Protocols	Step 1	15	
	Step 2	15	
	Step 3	15	
	Step 4	15	
	Step 5	15	
	Step 6	25	
	Total Score	**100**	